THE JUSTICE PROJECT

by
OXFORD PRO BONO PUBLICO*

for
JUSTICE UK

Legal Opinion on

Intercept Communication

University of Oxford, January 2006

*Oxford Pro Bono Publico is a programme run by the Law Faculty of the University of Oxford, an exempt charity (and a public authority for the purpose of the Freedom of Information Act). The programme assists solicitors and barristers who are themselves acting on a pro bono basis in the preparation of materials for legal work which they undertake for the public good or in the public interest. The programme does not itself provide legal advice, represent clients or litigate in courts or tribunals. The University accepts no responsibility or liability for the work which its members carry out in this context. The onus is on the solicitors or barristers in receipt of the programme's assistance to establish the accuracy and relevance of whatever they receive from the programme; and they will indemnify the University against all losses, costs, claims, demands and liabilities which may arise out of or in consequence of the work done by the University and its members.

TABLE OF CONTENTS

INTRODUCTION

This opinion evaluates the adequacy of the UK position on intercept communication through a comparative analysis of the use of intercept evidence in four jurisdictions namely New York (USA), Canada, South Africa, and Israel. 'Intercept evidence' is the shorthand term used to describe evidence gained from interception of telephone, internet or postal communications by the police or other authorised public body. It is to be distinguished from other kinds of evidence that may be gained by surveillance, including the bugging of cars and residences and the use of covert human intelligence.

The opinion examines the different legislative arrangements concerning intercept communication. In particular, the research focuses on the following questions:

- the circumstances in which interception of communication is allowed;
- the admissibility of such evidence in court proceedings;
- whether the admissibility of evidence depends on the legality of the interception of communication;
- means available to allow the defendant access to intercepted evidence at trial; and
- means available to protect the informants, police and secret methods.

The research commences with a summary of the UK position and then proceeds to look at the approaches of New York, Canada, South Africa and Israel. The various jurisdictional sections consider case law, legislation and legal scholarship.

PART I – INTERCEPT COMMUNICATIONS IN UK

As far as English Law is concerned, the interception of communications is mostly regulated by the *Regulation of Investigatory Powers Act 2000*[1] (hereinafter 'RIPA'). The scheme laid out by RIPA and a relation of some of the problems identified in it will be considered below, immediately after a brief account of the evolution of intercept communications in English Law.

A. Historical Background

English Law's position on intercept communications has been shaped to a great extent by two factors: the evolution of European human rights on the matter and the rise of new communications technologies in the last decade of the 20th Century. Since 1985, Parliament has answered the challenges posed by this subject through legislation. For better or for worse, out of this legislation and the traditions preceding it there has arisen a very distinct conception on the use of intercept communications in criminal trials and its place in law enforcement.

Traditionally, the interception of communications has been used as a way of detecting and preventing crime rather than prosecuting it in the UK.[2] Whilst under the Common Law the use of such evidence was not of itself inadmissible,[3] the practice still remained that the contents of intercept communications were not brought to trial directly, but rather served as an information-gathering tool for law enforcement agents: their use as an 'evidentiary' tool was always superseded by their use as an 'intelligence' tool.[4] Furthermore, before 1985 the interception of communications in England and Wales was not regulated by legislation. Rather, interceptions were regulated indirectly by the Post Office Acts[5] and directly by Home Office guidelines.[6]

In 1984, however, the European Court of Human Rights, in *Malone v the United Kingdom*,[7] held the law of England and Wales violated the European Convention on

---

[1] 2000 c. 23.

[2] *R. v Preston*, [1994] 2 A.C. 130, 142, 147; *Attorney General's Reference No. 5 of 2002* [2005] 1 AC 167, 174.

[3] R Cross and C Tapper, *Cross and Tapper on Evidence* (10th edn LexisNexis, London 2004) 546, citing *R v Derrington* (1826) 2 C & P 418 [interception of mail] and *R v Keeton* (1970) 54 Cr App Rep 267 [use of recorded telephone conversation as evidence in divorce trial].

[4] D Ormerod and S McKay, 'Telephone Intercepts and Their Admissibility' (2004) Criminal Law Review 15, 31.

[5] This even after the function of telephone operator was taken away from the Post Office through the *British Telecommunications Act 1981* (c. 38) by creating British Telecom as a separate corporate entity.

[6] N Taylor, 'Policing, Privacy and Proportionality' (2003) European Human Rights Law Review Supp (Special Issue) 86, 91.

[7] *Malone v the United Kingdom* (1984) 7 EHRR 14 [79].

Human Rights ('the European Convention').[8] The authority vested in the Home Office, though widely accepted, was deemed 'somewhat obscure and open to differing interpretations.' Because of this, the guidelines could not be regarded as 'an interference' 'prescribed by Law'[9] with the right to privacy protected in Article 8 of the Convention.

The defects reflected in *Malone*[10] were met by Parliament through the enactment of the *Interception of Communications Act 1985*[11] (hereinafter 'the 1985 Act'). This was the first legislative instrument dealing specifically with intercept communications in the United Kingdom. The authority to issue warrants of interception remained within the authority of the corresponding Secretaries of State.[12] Furthermore, the 1985 Act preserved the historical approach of using interceptions 'for the purpose of preventing or detecting serious crime'[13] and later to destroy the evidence obtained for this, as soon as retention was deemed unnecessary.[14]

With time, the 1985 Act was repealed. Many reasons led to this:

- The evolution and popularisation of new technologies and means of communication not considered in the 1985 Act, such as the Internet and mobile telecommunications.[15]
- The enactment of the Human Rights Act in 1998 (c. 42),[16] which incorporated the European Convention's right to privacy into the Law of England and Wales, a notion hitherto non-existent in the sense of the European Convention.[17] Under the European Convention, the interception of telecommunications represents an interference with the right to privacy.[18] Any breach of European Convention

[8] Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 (1953) 213 UNTS 222.

[9] This is a requisite of article 8.2 of the Convention, dealing with the right to privacy and of all of the Convention's freedoms. Cf. *Malone* (n 7); Cf. *Leander v Sweden* (1987) 9 EHRR 433.

[10] Ormerod and McKay (n 4) 19.

[11] 1985 c. 56.

[12] 1985 Act, s. 2.

[13] 1985 Act, s.2(2)(b).

[14] 1985 Act, s. 6(3).

[15] Cf. C Walker, 'Email Interception and RIPA: The Court of Appeal Rules on "The Right to Control" Defence' (2006) Communications Law, 2006 WL 1652477 (UK).

[16] Ormerod and McKay (n 4) 19.

[17] *R. v Brown* [1996] 1 All ER 545, 556 (Lord Hoffmann): 'English common law does not know a general right of privacy and Parliament has been reluctant to enact one.'

[18] Cf. *inter alia*: *Kruslin v France* (1990) 12 EHRR 547 [25-26]; *Kopp v Switzerland* (1998) 27 EHRR 91 [22]; *Lambert v France* (2000) 30 EHRR 346 [21].

privacy standards in intercepting communications would thus be 'unlawful'[19] and liable to be declared incompatible with the European Convention by the courts.[20]

- A new defeat for the Government before the European Court of Human Rights in Strasbourg in the case of *Halford v the United Kingdom* in 1997.[21] This case turned on whether the complainant had a right to privacy under the European Convention in the use of private (ie non-public) telecommunications systems, not regulated by the 1985 Act, which the Court answered in the affirmative. On this view, the 1985 Act did not enact a 'comprehensive scheme to regulate the whole field of interception,' but rather to regulate cases similar to that of *Malone*.[22] Thus s.1 only made an offence the interception of communications when carried out through public telecommunications systems,[23] not private ones. As this area was devoid of legislation, the interference with the right to privacy was not carried out 'in accordance with the law,' as required by article 8(2) of the European Convention.
- The 1985 Act was thus replaced by RIPA. In essence, RIPA covers more situations than the 1985 Act, although in more than one respect, the 1985 Act's regime remains intact.

B. English Legislation

Regulation of Investigatory Powers Act is 'long' and at times 'perplexing'.[24] Although it has been hailed as 'a huge step forward'[25] in upholding the European Convention's norms and case-law, the overall evaluation of the Act among commentators and courts has not been as enthusiastic. Like the 1985 Act, it could be argued RIPA still strives to prohibit the use of the fruits of intercept communications as evidence before courts. Part I of RIPA deals with both the interception of postal and telecommunications and the acquisition of 'communication data.' Part II deals with surveillance and covert

[19] Human Rights Act 1998, s. 6(1).

[20] Ibid, s. 4(1). Perhaps more significantly, the Human Rights Act also mandates the Courts to take into account the Case-Law of the European Court of Human Rights (s.2(1)(a)), some of whose judgments will be used below.

[21] *Halford v the United Kingdom* (1997) 24 EHRR 523; Cf. Ormerod and McKay (n 4) 19. One of Halford's two telephone lines in her office, not falling within the definition of 'public' telecommunications system under the 1985 Act, was intercepted for the purpose of obtaining information against her. This information was sought by members of the Merseyside Police Authority regarding a law suit initiated by Ms. Halford against the Chief Constable of Merseyside and the Home Secretary, as she, a police officer, alleged to have been denied promotion several times solely on account of her being a woman.

[22] Ibid.

[23] 'Public' telecommunication systems were those which were run pursuant to s. 4(1) of the *Telecommunications Act 1984* (c.12, now repealed by the *Communications Act 2003*, c. 21) and designated as such by the Secretary of State. 1985 Act, s. 10(1).

[24] *Reference No. 5* (n 2) 178 (Lord Bingham).

[25] Taylor (n 6) 92.

intelligence sources, which overlap to some extent with the topics which form part of this consultation.

Under RIPA, it is both a punishable offence[26] and a tortious act[27] to 'intercept' without lawful authority any communications in the course of transmission through a public postal system, a public telecommunications system[28] or a private telecommunications system.[29] The notion of 'interception', however, overlaps with other notions covered by the Act, resulting in a number of practical implications under both RIPA and the European Convention. This overlap has important consequences as regards the admissibility scheme.

The simplest definition of interception is perhaps given by Amanda Hale and John Edwards,

> A person intercepts a communication in the course of its transmission if, as a result of his interference in the system or monitoring of the transmission, some or all of the contents are made available, while being transmitted, to a person other than the sender or the intended recipient of the communication.[30]

Furthermore, it is noteworthy that RIPA fictively considers an interception as carried out in the course of its transmission when (i) it is stored so that the **recipient** can access and collect it later[31] and (ii) when the contents of the transmission are stored by the **interceptor** so as to make them available after the transmission ('subsequently').[32]

In some cases a conversation overheard or a message read by law enforcement agents is not 'intercepted' but rather *surveyed*. '**Surveillance**' activities are regulated by

[26] RIPA, ss. 1(1) and 1(2).

[27] RIPA, s. 1(3).

[28] Under RIPA, s. 2(1)), a 'telecommunications system' includes the apparatus attached to it (i.e. the phones themselves) and 'telecommunications service' consist of providing access the telecommunications systems. Thus a telecommunications system would include a telephone apparatus, whereas a telecommunications service includes the landline to which it is connected. 'Public telecommunication system' is any part of a *public telecommunications service* as are located in the United Kingdom. Public telecommunications service, on the other hand, is any telecommunications provided to all or part of the public anywhere in the United Kingdom. Thus an example of a *public telecommunications system* would be the payphones in the streets.

[29] This last notion remedies in part the deficiency of the 1985 Act discussed in *Halford*. It is defined as a non-public telecommunications system attached directly or indirectly to a public telecommunications system with apparatuses which are both (i) located in the United Kingdom and (ii) used to make the attachment to the public telecommunications system (s.2(1)). An example: telephone systems in any regular office, provided they are connected to a public telecommunications service (such as British Telecom's).

[30] A Hale and J Edwards, 'Getting it Taped' (2006) 12 Computer and Communications Law Review 71; Cf. RIPA, s. 2(2).

[31] RIPA, s. 2(7).

[32] RIPA, s. 2(8); Hale and Edwards (n 30) 71.

Part II of RIPA. With regards to what is relevant for the purposes of this paper,[33] surveillance[34] occurs when any party to the communication surveyed consents to its being overheard or read by law enforcement agents. This particular form of surveillance is called *directed surveillance*.[35]

Consent plays a major role in distinguishing between an intercepted communication and a surveyed communication. In the case of 'surveillance' one of the parties to the conversation has given consent to its being overheard. Whilst both kinds of conduct constitute in essence the same exercise (that of overhearing or reading a communication belonging to an unsuspecting party), the authorisation and admissibility regimes are considerably different for both, all of which has implications on the right to privacy.

At first sight, the distinction appears useless. The object of this paper being 'intercepted' communications, there appears to be no place for surveillance here. As simple as it seems, this distinction is key to understanding the whole of RIPA's authorization, admissibility, and privacy protection schemes.[36]

Surveyed communications should not be rejected wholesale when dealing with intercepted communications. Surveyed communications become relevant when examined within the context of the European Convention of Human Rights, under which there is support for the notion that when the recipient has consented to intercept a call, the other parties to such communications do not lose all of their right to privacy.[37] As the right to privacy exists for both cases, it appears RIPA separates two notions which under the

---

[33] Surveillance activities cover a number of situations besides the overhearing or reading of communications. For instance, surveillance covers the use of devices to record all that happens inside residential premises or private vehicles. RIPA, s. 26(3).

[34] RIPA, ss. 48(4) and 26(4)(b).

[35] Surveillance may be directed or intrusive. "Intrusive" surveillance is one carried out by a person or a device with the purpose of recording all that happens in residential premises or in a private vehicle (Cf. RIPA, s. 26(3)). Surveillance is "directed" when carried out for the purposes of a specific investigation whenever such surveillance has not been a forced response to events making it "reasonably" impractical to obtain authorisation. Moreover, for surveillance to be directed, one of its likely results is obtaining of private information about a person (Cf. RIPA, s. 26(2)). One practical difference is that the number of officials entitled to authorise "intrusive" surveillance is less than those who authorise directed surveillance.

[36] Ormerod and McKay (n 4) 19.

[37] Cf. *A v France* (App no 14838/89) ECHR Series A no 237-B [36]; *M.M. v the Netherlands* (App no 39339/98) ECHR 8 April 2003 [40-43]: '40. In the present case, which like the A. v France case is characterised by the police setting up a private individual to collect evidence in a criminal case, the Court is not persuaded by the Government's argument that it was ultimately [*the undercover individual*] who was in control of events. To accept such an argument would be tantamount to allowing investigating authorities to evade their responsibilities under the Convention by the use of private agents. (…) 41. It is not necessary to consider the Government's suggestion that Mrs S. would have been fully entitled to record telephone calls from the applicant without the involvement of public authority and use the recordings as she wished, the issue in this case being precisely the involvement of public authority. (…) 42. There has accordingly been an 'interference by a public authority' with the applicant's right to respect for his 'correspondence'. (…) 43. Such an interference will violate Article 8 of the Convention unless it is 'in accordance with the law', pursues one of the 'legitimate aims' set out in the second paragraph of that Article, and can be considered 'necessary in a democratic society' in pursuit of that aim.'

European Convention appear to be the same: overhearing and accessing the communications of an unsuspecting party.

This is important because RIPA establishes a significantly lower threshold for situations when a party consents when compared to intercepted communications properly so called. 'Intercepted' communications must be authorised by a warrant issued by a Secretary of State[38] at the request of authorised officials.[39] The Secretary of State 'shall not' issue this warrant except when satisfied of the existence of certain limited grounds.[40] By contrast, when only one party consents, RIPA allows for non-warrant authorisation.[41] All types of surveillance are authorised by a wide number of officials[42] without any formal requirements. They can be authorised when they 'believe' that such authorisation is required on certain grounds.[43] This difference of language between 'shall not' and 'believes'[44], not to mention the discretion given to law enforcement agents, suggests the difference in threshold is indeed great.

Accordingly, it is arguable that situations so similar may not warrant such a drastic reduction of guarantees for all cases. In short, that this reduction is disproportionate and that the right to privacy of the unsuspecting party to a surveyed communication is not being properly respected by RIPA.

Finally, neither warrant, nor non-warrant authorizations are issued by judges in English Law. This is at odds with the European Convention's requirements –at least as it is interpreted by the European Court of Human Rights- that authorisations to intercept be

[38] RIPA, s. 5.

[39] RIPA, s. 6. Such officials are: the Chiefs of the Intelligence and Security Services, the Director of GCHQ, the Director General of the National Criminal Intelligence Service, the Commissioner of Police of the Metropolis, the Chief Constable of the Royal Constabulary of Ulster, the chief constable of any police force ruled by the *Police (Scotland) Act 1967* (c. 77), the Commissioners of Customs and Excise, the Chief of Defence Intelligence, any authorised by a treaty to do this.

[40] RIPA, s. 5(3). They include the preservation of national security, safeguarding the economic well-being of the United Kingdom, among others. More significantly, such grounds include the detection and prevention of 'serious crime', the traditional uses of interception in the United Kingdom. RIPA interprets 'serious crime' as any offence which would entail three or more years of prison when committed by persons of 21 years of age or older without previous convictions. Alternatively, 'serious crime' is any offence committed by means of violence or one which involves 'substantial financial gain' or one carried out by a group of people with a common purpose. Cf. RIPA, ss. 81(2)(b) and 81(3).

[41] RIPA, s. 3(1) and 3(2).

[42] RIPA, s. 28. The list is appended to RIPA as Schedule I and comprises officials ranging from any police force, to any of the Intelligence Services, any of the Armed Forces, the Commissioner of both Customs and Excise and Revenue, the Home Office, the Post Office, local authorities, the Department of Health and NHS trusts.

[43] This if they 'believe' that the authorisation is necessary for protecting the interests of national security, preventing or detecting crime, safeguarding the economic well-being of the United Kingdom, preserving public health, collecting taxes, among others. RIPA, s. 28(3).

[44] Ormerod and McKay (n 4) 28-29. They also contrast the use of the terms 'serious crimes', binding the Secretary of State for issuing interception warrants, and the general use of the word 'crime' for surveillance authorizations. Cf. s. 5(3)(b) with 28(3)(b), 29(3)(b) and 32(3)(b).

ideally issued or controlled by judges[45] and not the ministers or law enforcement agents, as is the case under RIPA.

C. Admissibility of Intercept Evidence under Regulation of Investigatory Powers Act

As stated previously, RIPA makes inadmissible in trial the use of evidence gathered by means of interception. The way it does this, however, is curious. Read in plain language, the Act does not seem to forbid that the fruits of interception may be included as part of evidence. What RIPA does is to prevent both the prosecution and the defence from questioning the provenance of intercepted evidence. The goal of this part of RIPA is to 'shroud in secrecy many of the workings of the process of investigation'[46] specifically in the case of intercepted communications.

This part of RIPA is very complex and merits more explanation. As stated above, both interception and surveillance overlap to a great measure. However, they are authorised differently. This is important because the purpose of the inadmissibility scheme described above appears to be that of protecting the 'warrantry regime'[47] (ie that of interception properly so called). This feature of RIPA is not new, as it was also included in Section 9 of the 1985 Act.

RIPA's sections 17 and 18 preserve in essence the regime of the 1985 Act as regards admissibility. In synthesis, s.17(1) makes it impossible to disclose at trial the content of any intercepted communication in a manner that tends to suggest that an interception warrant exists or has been applied for, among others.[48] S. 17(1) also forbids disclosing the communication at trial tending to suggest a wide range of persons[49] has committed unlawful interception. This is all carried out by means of forbidding the asking of questions, adducing of evidence and even asserting that any of the actions described before have happened.

This is perhaps better explained by way of example. Let us suppose the police forces have overheard conversations of two non-consenting parties. If the police carry out actions according to RIPA, they will have procured authorisation by the relevant principal Secretary of State for the relevant functions on the basis of the limited grounds enumerated in s. 5 (e.g. the Home Secretary for matters dealing with national security). Should this happen, the existence of the warrant must remain secret. In these

---

[45] Cf. *Klass and Others v Germany* (1979-80) 2 EHRR 214, [56]; *Huvig v France* (1990) 12 EHRR 528 [33]; *Kopp* (n 18) [74].

[46] P Mirfield, 'Regulation of Investigatory Powers Act 2000: Part 2: Evidential Aspects' (2001) Criminal Law Review 91.

[47] *Reference No. 5* (n 2) 182.

[48] RIPA, ss. 17(1) and 17(2).

[49] They include any person to whom the whole of RIPA's chapter I is addressed, any member holding office under the Crown, (inserted by any person employed by police forces, postal services or for public telecommunications services. They also include the providers of postal and public telecommunication services and any member of the staff of the Serious Organised Crime Agency (inserted by the Serious Organised Crime and Police Act 2005 (c. 15) s. 59 and Schedule 4). RIPA, s. 17(3).

circumstances, a prosecutor could rely on this evidence to secure convictions, because when he or she presents it in Court as 'intercepted evidence', he or she would give away the fact that a warrant has in fact been issued or should have been issued.

S. 17 thus appears more convenient to the defendant than to the prosecution. However, this is not the case. Firstly, the prohibition works both ways: the defendant could not benefit from exculpatory intercepted evidence either, as using this intercepted evidence will imply the existence of the interception warrant.[50]

Additionally, RIPA does allow for disclosure only to the prosecutor of the contents of interception, even if not useable at trial,[51] to the extent necessary to carry out his duty to secure the fairness of the prosecution. Regardless, as Peter Mirfield points out,[52] this breaks the principle of equality of arms arising out of Article 6 of the European Convention[53] requiring that neither side be placed at a disadvantage in relation to the other.[54] The prosecution is indeed obliged to ensure the fairness of prosecutions under s. 18(2)(a), as in all cases. However, RIPA denies at all times to the defence access to the products of interception.[55] Thus as Mirfield points out,[56] unlike non-RIPA cases, where the prosecution has a duty of disclosure to the defence,[57] RIPA forbids the defence access to intercepted communications. This disadvantage is even graver when the intercepted material is equivocal, because the fairness of the prosecution might be perceived less clearly.[58]

It must be noted, however, that as interpreted by the House of Lords s. 17 has been given an interpretation which is arguably different than that of the Act's text,[59] but which according to their Lordships is more in accordance with a purposive interpretation of RIPA. In *Attorney General's Reference No. 5 of 2002*, their Lordships interpreted s.17 as not totally precluding enquiries as to the way the interception was carried out. As put by Lord Bingham, that

> [D]isclosure is not prohibited if the interception was lawfully authorised under those sections. It would be absurd to conclude that there could be no inquiry to establish whether the interception was lawfully authorised or not, and whether or not the interceptor's conduct was excluded from criminal liability under section 1(6). In a civil claim under section 1(3) such an inquiry would be inevitable. Given the obvious public

[50] *Mirfield* (n 46) 91.

[51] Cf. RIPA, s. 18(7)a.

[52] *Mirfield* (n 46) 96.

[53] This article deals with the fair trial issues.

[54] *Ankerl v Switzerland* (App no 17748/91) ECHR 1996-V [38]; *Foucher v France* (1997) 25 EHRR 234 [34]; *Roux v France* (App no 16022/02) ECHR 25 April 2006 [23].

[55] There is no equivalent to s. 18(7)(a) for the defence.

[56] *Mirfield* (n 46) 96-97.

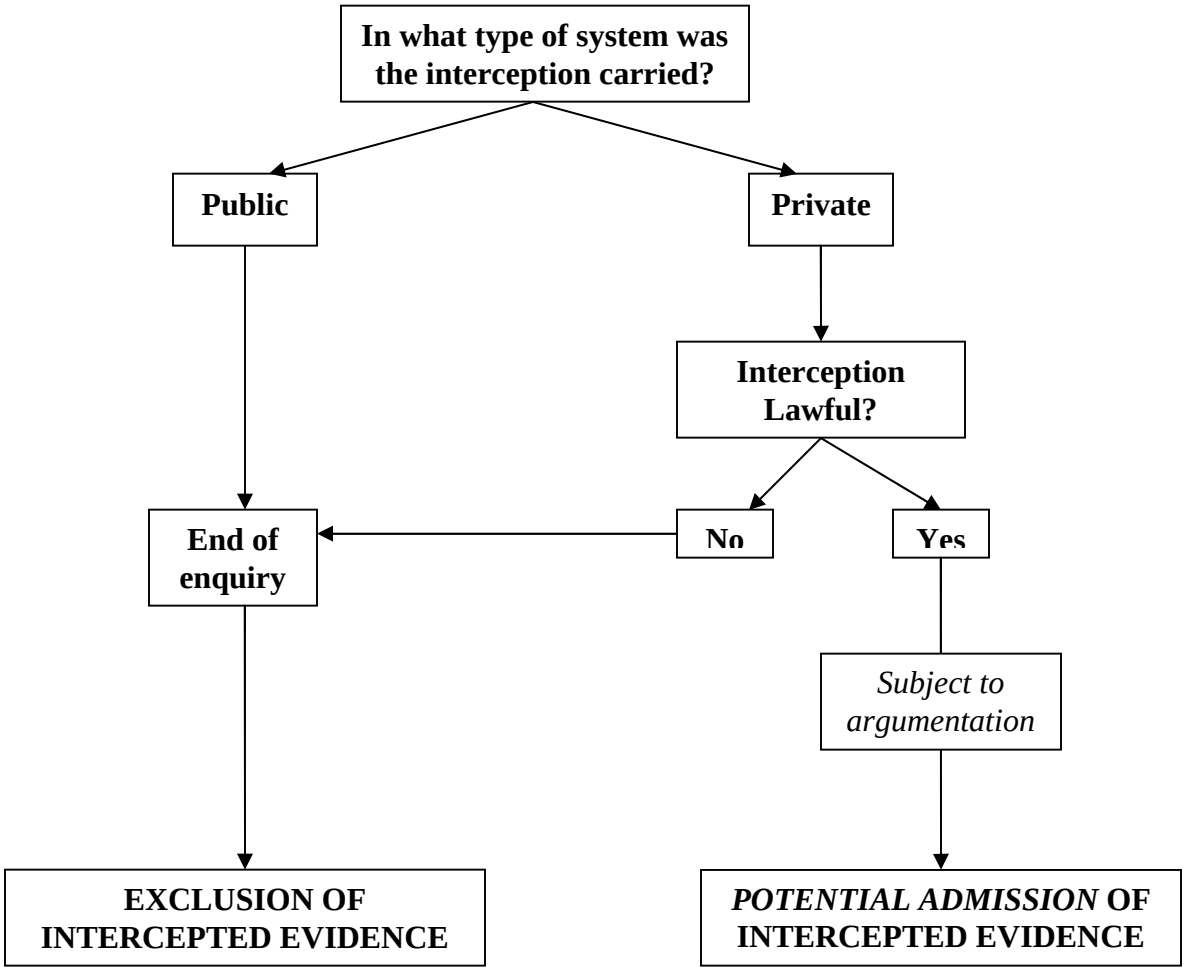
[57] This under the *Criminal Procedure and Investigations Act 1996* (c. 25) ss. 3(1)(a) and 7A(2) (inserted for England and Wales by s. 37 of the *Criminal Justice Act 2003* (c. 44)).

[58] *Mirfield* (n 46) 96.

[59] Ibid.

> interest in admitting probative evidence which satisfies the requirements of sections 1(6), 3 and 4, and the absence of any public interest in excluding it, I am satisfied that a court may properly inquire whether the interception was of a public or private system and, if the latter, whether the interception was lawful. If the court concludes that it was public, that is the end of the inquiry. If the court concludes that it was private but unlawful, that also will be the end of the inquiry. If it was private but lawful, the court *may* (subject to any other argument there may be) admit the evidence.[60] [Emphasis added]

The test limited enquiry system may be summarised thus:



Finally, it must be pointed out that the inadmissibility established by s. 17 does not reach communications surveyed with the consent of one of its parties.[61]

[60] *Reference No. 5* (n 2) 182 (Lord Bingham), Cf. 185 (Lord Nicholls) [holding such enquiries 'essential to the conduct of a fair trial' and harmless to the warrant system], Cf. 185-186 par. [31] (Lord Steyn).

[61] As they are authorised by s. 3, they are expressly excluded from s.17's ban by RIPA's s. 18(4).

D. Conclusion

The scheme established in English law for admitting evidence at trial is rather cumbersome. It forbids indirectly the use of intercept evidence at trials by making it impossible for defendants or prosecutors to put in evidence the means through which this evidence has been acquired. The justification for this is the protection of the warrant system: keeping secret the State's methods of investigation. Nevertheless, the case law evidences a growing tendency among judges that such a burdensome prohibition and the approach to intercepted communications does not contribute to safeguard the warrant system and is thus unnecessary.

RIPA also creates asymmetries. The defendant is the one party with most to lose here. The defendant is never allowed to examine the content of intercept communications. The normal duties of disclosure by prosecutors do not apply in RIPA, leaving the defendant at a loss of means of defence.

In simple words, the greatest problem of RIPA is one of focus. It preserves reliance in intercepted communications as an intelligence-gathering method in fighting crime, and not as an evidential tool. In sum, it pretends to be used as evidence indirectly: as indicia pointing out to occurrence of facts, but not as proof of them. In order to accommodate such goals, RIPA establishes a very complex system which confounds all participants of the legal system. Its wording is anything but straightforward. There is significant overlapping between activities such as 'interception' and 'surveillance', which only make sense if RIPA is viewed in isolation. There is concern for the way privacy and fair trial issues are being dealt with under RIPA.

As will be seen below, other systems of law adopt and allow for disclosure at trial without weakening their law enforcement efforts because of this. When considered in the context of existing human rights protections, RIPA can be found lacking in more than one respect. A decision to keep or modify RIPA should therefore bear in mind whether disclosure really damages the warrant system as it is assumed at present and whether other methods exist which could preserve the warrant system in good order without unduly burdening the human rights guarantees safeguarded by English law.

PART II – APPROACHES OF OTHER COUNTRIES

I. The Admissibility of Intercept Evidence in New York (USA)[62]

The State of New York offers an interesting example on the use of intercept communications. New York State Law, under the aegis of both the Federal and State Constitutions, attempts to balance the protection of privacy rights and fair trial values with the use of intercept evidence as a prominent tool in detecting and prosecuting organised crime. As a major industrial port and communications hub, New York has had to deal with a plethora of organised crime families and with sophisticated criminal networks dealing with everything from gambling to narcotics and more recently with terrorism.

The State's Law on intercept communications is characterised by an interaction between Federal Law and State Law, the former prevailing over the latter in case of conflict. As with any State in the American Union, New York has significant leeway to regulate all matters not delegated upon the Federation.[63] The interception of communications, however, is a matter of Federal regulation. As the unlawful use of such a tool would imply, among others, invading the constitutional right to be free from unreasonable searches and seizures,[64] the regulation of interceptions falls within the purview of the competence of the Union.[65] As a result of this, any State Legislation implying a more invasive regime of interception than the one enacted by the Federal Congress 'runs afoul of the supremacy clause,'[66] and is thus null and void.

---

[62] This section has been greatly benefited by the use of *McKinney's Consolidated Laws of New York Annotated*, which have served as a constant and invaluable primary and secondary source of referencing throughout.

[63] *Constitution of the United States of America* ('*US Constitution*'), 10th Amendment: 'The powers not delegated to the United States by the Constitution nor prohibited by it to the States, are reserved to the States respectively, or to the people.'

[64] Cf. *Berger v New York* (1967) 388 US 41 (SC) (Fed), 53 ff. US Constitution, 4th Amendment: 'The right of the people to be secure in their persons, Houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by oath, or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.' (Emphasis added)

[65] *US Constitution* (n 633), 14th Amendment § 1: 'All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property without due process of law; nor deny to any person within its jurisdiction the equal protection of the Laws.' (Emphasis added).

[66] *People v Shapiro* (1980) 431 N.Y.S.2d 422 (CA), 431; P Preiser, 'Practice Commentaries' in *McKinney's Consolidated Laws of New York Annotated*, Commentary to art. 700.05; Cf. *US Constitution* (n 633), Article VI § 2: 'This Constitution and the Laws of the United States which shall be made in pursuance thereof; and all Treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the Contrary notwithstanding.' (Emphasis added).

Thus, as will become apparent later, New York Law on intercept communications mirrors Federal Legislation. Furthermore, Federal Case Law[67] can and will be cited alongside New York Case Law.[68]

A. Evolution of New York Legislation

The evolution of intercept communications in New York has been driven by developments in Federal case law first, and Federal legislation, later. In turn, changes in both Federal case law and legislation have been met by the State Legislature with Statutes containing such changes.

i. State Constitution

The first regulation of interceptions in New York's legal system was enacted in 1938. Article I of the State's Constitution was modified so it would read, in relevant part:

> The right of the people to be secure against unreasonable interception of telephone and telegraph communications shall not be violated and ex parte orders or warrants shall issue only upon oath or affirmation that there is reasonable grounds to believe that evidence of crime may be thus obtained, and identifying the particular means of communication and particularly describing the person or persons whose communications are to be intercepted for the purposes thereof.[69]

In pursuance of this modification to the State Constitution, the State Legislature added section 813-a to the Code of Criminal Procedure in 1942 and amended later in 1958.[70] This section regulated all matters regarding interception of communications until 1967, when the Supreme Court of the United States decided, in *Berger v New York*, that § 813-a was unconstitutional as it stood.

ii. Federal and State Laws

Before *Berger*, Federal case law had held[71] that the Fourth Amendment to the Constitution only provided protection against unreasonable searches and seizures of material things – 'houses, papers and effects'- and not against the overhearing of a

---

[67] Federal Case-Law will be properly identified as '(Fed)' in each case for the convenience of the reader. The names of the federal tribunal will be abbreviated thus: the United States Supreme Court will be 'SC US', the Federal Courts of Appeals will be 'CA', the District Courts will be cited in the normal way (e.g. "E.D.N.Y" is the Federal District Court for the "Eastern District of New York").

[68] New York tribunals will be abbreviated thus: the State's Court of Appeals will be (this is the State's highest Court, never to be confused with the *Federal* Courts of Appeal), the Appelate Division of the State's Supreme Courts will be 'SC, App Div' followed by the number the Department issuing the order, the county-level parts of the Supreme Court will be 'SC', and the County Courts will be 'CC', followed the name of the county where each sits.

[69] *Constitution of the State of New York*, Art. I § 12. *Cited in* 'Electronic Eavesdropping under the Fourth Amendment—after *Berger* and *Katz*' (1967-1968) 17 Buffalo Law Review 455, 466.

[70] 'Electronic Eavesdropping' (n 69) 466.

[71] *Olmstead v United States* (1961) 277 US 438 (SC US) (Fed).

conversation, which is intangible.[72] Presumably as a response to this,[73] the Federal Congress enacted the *Federal Communications Act*,[74] which forbade the use in federal trials of intercept evidence not acquired on the basis of a warrant.[75] The tangible/intangible divide was later overruled,[76] and the inadmissibility of evidence obtained in violation of the Fourth Amendment was deemed applicable not only in Federal but in State Courts as well.[77] It is on the basis of this evolution that *Berger* arose.

Section 813-a of New York's Code of Criminal Procedure allowed for many actions ruled as contrary to the Fourth Amendment in *Berger*. For instance, no probable cause needed to be shown for renewing the eavesdropping warrants, nor were there controls that once the evidence sought was obtained the interception of communications should be stopped. As interception of communications was deemed an invasion upon privacy 'broad in scope',[78] s. 813-a's lack of attention to detail and particularization made it unconstitutional.

In response to Berger and the later decision of *Katz v United States*,[79] the Federal Congress enacted the *Omnibus Crime Control and Safe Streets Act of 1968* (Pub. L. 90-351) Title III[80] of which established a system regulating electronic eavesdropping.[81] As a result, New York enacted its own version of this Act in 1969, later carried over to the State's *Criminal Procedure Law*[82] ('CPL') when the latter was enacted.

---

[72] *Olmstead* (n 711) 466 ['Neither the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been violated as against a defendant, unless there has been an official search and seizure of his person or such a seizure of his papers or his tangible material effects or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure…']

[73] The *Olmstead* doctrine became unpopular in the United States. Cf. 'Electronic Eavesdropping' (n 69) 457-458.

[74] 47 USC ch. 5.

[75] 47 USC § 675.

[76] *Irvine v California* (1954) 247 US 128 (SC US) (Fed).

[77] *Mapp v Ohio* (1961) 367 US 643 (SC US) (Fed).

[78] *Berger* (n 644) 56.

[79] *Katz v United States* (1967) 389 US 347 (SC US) (Fed). This decision held the Fourth Amendment could be violated even if there is no trespass in the placement of devices serving to intercept communications. This trespass standard was also a result of *Olmstead* and was expressly laid down in *Goldman v United States* (1942) 316 US 129 (SC US) (Fed), wherein the placement of electronic devices capable of overhearing conversations was held not to violate the Fourth Amendment because the federal agents involved in the operation had committed no trespass on the property of those whose conversations were overheard. In reversing *Goldman* and what was left of *Olmstead*, Stewart J, writing for the Court, established that the Fourth Amendment protects persons, not places, and thus it was not correct to circumscribe Fourth Amendment protection only to physical spaces.

[80] 18 USC 2510-2520.

[81] Preiser (n 666).

[82] As the name implies, this law regulates the procedure for criminal trials in the State of New York.

However, both the Federal and State Statutes covered only 'wiretapping'[83] and 'bugging'.[84] Advances in technology, however, determined that by the 1980s a change was needed. As a result of this, Congress enacted the Electronic Communications and Privacy Act of 1986 (Pub. L. 99-508). In turn, in 1988 the State of New York enacted *Penal Law*[85] article 250[86], modified CPL articles 700[87], 710 and 720, and created article 705 CPL dealing with 'pen registers'[88] and 'trap and trace devices.'[89] The 1988 legislation, amended several times, rules the interception of communications in the State of New York up to this day.

B. Admissibility of Intercept Evidence under the Criminal Procedure Law

For what is relevant for the purposes of this paper, under New York Law, a communication is 'intercepted'[90] in any of the following situations:

- In cases of telephonic[91] or telegraphic communications, when they are intentionally overheard or recorded by a person other than the sender/receiver by means of any 'instrument, device or equipment';
- In cases of electronic communications,[92] when they are accessed (overheard, recorded, stored, etc.) by a person other than the sender or receiver.[93]

---

[83] Broadly speaking, it refers to the interception of telephone lines by means of a device ('tap') enabling conversations to be heard.

[84] Broadly, overhearing conversations by the use of devices such as microphones ('bug'), inserted within hearing range of the places where such conversations are taking place.

[85] This is the general criminal law code of the State of New York, a compilation of the substantive aspects of criminal law (definition of offences, etc.).

[86] This article creates, among others, the offences of eavesdropping (205.05), possession of eavesdropping devices (205.10) and tampering with private communications (205.25).

[87] This deals with interception and use of evidence at trial.

[88] Devices used to know the number corresponding to incoming phone calls. CPL, Art. 705.

[89] Used to locate a user on the basis of the signal emitted by the communications device employed by him/her. CPL, Art. 705.

[90] CPL, Art. 700.05[3].

[91] Under article 250.00[4] of the Penal Law 'telephonic communication' means any *aural transfer* made in whole or in part by the aid of wire, cable or other means furnished by a provider of such services (i.e. a telephone company).

[92] Under article 250.00[5] Penal Law, 'Electronic Communications' are defined as any transfer of signs, signals, writing, images, sounds, data or 'intelligence of any nature' by means of wire, radio, electromagnetic, photo-electronic or photo-optical systems. *Excluded from this definition*, however, are telegraphic and telephonic communications, as well as those relayed in a way that makes them accessible to the general public, among others.

[93] CPL, Art. 700.05[3] and Penal Law, Art. 250.00[6]: ' 'Intercepting or accessing of an electronic communication' and 'intentionally intercepted or accessed' mean the intentional acquiring, receiving, collecting, overhearing, or recording of an electronic communication, without the consent of the sender or intended receiver thereof, by means of any instrument, device or equipment, except when used by a telephone company in the ordinary course of its business or when necessary to protect the rights or property of such company.'

In either case, interception only occurs when either the sender or the receiver has not consented to its overhearing or recording.[94] If there is consent by the sender or the receiver, no 'interception' occurs and thus no warrant is needed to use the evidence obtained at trial.[95]

Under New York Law, eavesdropping statutes are strictly construed due to the invasiveness of interceptions in the privacy of the subjects concerned.[96] It is necessary for law enforcement officials to strictly comply with all requirements laid down by the Law on this matter. The burden of proving compliance with the statutes thus rests with the prosecution.[97]

The general principle of admissibility is enunciated by Article 700.70 of the CPL, which reads, in relevant part,

> The contents of any intercepted communication, or evidence derived therefrom, may not be received in evidence or otherwise disclosed upon a trial of a defendant unless the people, within fifteen days after arraignment and before the commencement of the trial, furnish the defendant with a copy of the eavesdropping warrant, and accompanying application, under which interception was authorized or approved.

From the outset, it is evident that there a significant difference between New York's approach and the United Kingdom's.

Facts known to the prosecution directly or indirectly because of intercepted communication may be admitted in evidence upon notification. *The logical implication is that the substance of the contents of any communication interception will be made available to both the prosecutor and the defendant*, who may question the propriety of every stage of the interception operation. Should the interception operation not comply with the requirements set out by the Law, the defendant may in principle move to suppress the evidence obtained illegally.

To this end, defendants are aided by the notification of the warrant and its application.[98] The application for the warrant and the warrant itself contain extensive information on the way the interception operation has been carried out. Therefore, this notification enables defendants to elucidate many grounds for suppression of evidence, should they deem it necessary.[99] It also alerts defendants to the existence of evidence

---

[94] The definition of 'interception' in article 700.05 CPL covers the use of terms 'wiretapping' (i.e. interception of telephone or telegraphic communications) and 'accessing' electronic communications in art. 250.05 Penal Law. In turn, paragraphs [1] and [6] of this article establish this lack of consent as a condition for both 'wiretapping' or 'accessing…' to take place.

[95] *People v Simmons* (1975) 384 N.Y.S.2d 367 (SC), 372-373; *People v Smith* (2 Dept) (1979) 415 N.Y.S.2d 68, 70.

[96] *People v Gallina* (1983) 466 N.Y.S.2d 414 (SC), 420; *People v Schulz* (1986) 67 N.Y.2d 144 (CA), 148-149; *People v Capolongo* (1995) 85 N.Y.S.2d 151 (SC), 165 ['bedrock principle']; *People v Darling* (2000) 720 N.Y.S.2d 82 (CA), 85.

[97] *People v Schulz* (n 966) 148; *Darling* (n 966) 85.

[98] CPL, Art. 700.70[1].

[99] *People v Capolongo* (1994) 609 N.Y.S.2d 926 (SC), 929; *People v Cruz* (1974) 357 N.Y.S.2d 709 (CA), 713.

which may be used against them in court. Lack of notification produces an irremediable[100] impossibility[101] to use intercepted communication as evidence.[102]

i. General Requirements for Suppression of Inadmissible Intercepted Evidence

On this view, evidence derived from intercepted communications may be suppressed if defendants meets certain legal requirements.

First, they must prove they have been 'aggrieved' by the interception operation.[103] In order to do this, defendants must prove that either they were a party to the conversation intercepted[104] or that they had a proprietary interest in the premises where the interception took place.[105] This first element is thus a question of *standing*. The fact that a person is a defendant in a criminal trial does not of itself[106] grant this person the right to move to suppress intercepted evidence.[107]

After showing themselves aggrieved, defendants must afford a ground for suppressing evidence. For example: that the judge issuing the warrant was not competent or that the interceptors could not legitimately enter X's or Y's premises in order to intercept their communications. Such grounds are too many to enumerate here and may range from the issuance by a higher court of a new precedent supporting defendant's motion, to allegations based on the facts of the situation at hand, etc. Nevertheless, New York Law lays down some requirements for every stage of the interception operation which could serve as grounds for suppression if not observed. They will be considered as 'particular' requirements for admissibility in the next section.

In sum, it appears that a defendant named by 'A' and 'B' in a conversation between them without being a party to such conversation cannot move to suppress it, as the defendant, not a party to the conversation, has not been aggrieved. This statement must be qualified, however, because pursuant to the case law all defendants are aggrieved

---

[100] *People v Capolongo 1995* (n 966) 165.

[101] *People v Hickey* (1992) 582 N.Y.S.2d 517 (SC), 518-519.

[102] Exceptionally, it is possible for the prosecution to request from the trial court the extension of the fifteen day period upon showing good cause for and lack of prejudice in such extension. CPL, Art. 700.70[2].

[103] Cf. CPL, Art. 710.20.

[104] *People v McDonough* (1996) 275 N.Y.S.2d 8 (CC Nassau), 12; *People v Konyack* (1984) 471 N.Y.S.2d 699 (SC, App Div 3 Dept), 700-701; *U.S. v Ragusa* (1984) 586 F.Supp 1256 (E.D.N.Y.) (Fed), 1258.

[105] *People v Sardegna* (1982) 457 N.Y.S.2d 123 (SC, App Div 2 Dept), 123; Cf. *People v Gallina* (n 966) 417 [lack of proprietary interest over telephone intercepted does not preclude moving to suppress if defendant is a party to conversation]

[106] *People v Wakefield Financial Corp.* (1992) 590 N.Y.S.2d 382 (SC) [defendants cannot challenge warrant absent standing]; *U.S. v Austin* (1975) 399 F. Supp 698 (E.D.N.Y) (Fed), 700, n. 1 [defendants not named in warrant nor overheard in communications intercepted lack standing].

[107] However, *only defendants have standing to suppress*. Cf. *Matter of Application for a Search Warrant No. L-18/81* (1981) 437 N.Y.S.2d 635 (Crim CC Kings), 639.

when the grounds for suppression enable this. For instance, the need to show prejudice is irrelevant if the observance of the chain of custody of the intercepted evidence has been breached at some point in a manner depriving it of all reliability. New York Law, for example, enjoins law enforcement agents to place before the judge issuing the eavesdropping warrant so that the latter may seal it. As will be seen later, the purpose of this is to ensure that the product of evidence has not been tampered with by law enforcement agents or prosecutors, assuring its reliability. Thus the lack of observance of this requirement will generally lead the evidence not duly sealed to be suppressed without showing prejudice.[108]

Finally, it goes without saying that suppressed evidence may not be used at criminal trials. What is noteworthy is that regardless of this, disclosure of intercept evidence is allowed in civil forfeiture actions[109] even if they are not admissible at criminal trial[110] provided the issuing judge has duly sealed the intercept evidence after having received it.[111]

ii. Particular Grounds for Suppression of Illegally Intercepted Evidence

New York Law regulates every stage of the interception operation. As seen above, any omission on the part of interceptors may potentially serve as a ground for suppression of evidence if defendants prove themselves 'aggrieved' by such omission. The most important of these requirements will be considered below, with regard to each stage of the interception operation.

(a) Requirements to be met before issuing Eavesdropping Warrants

At the outset, it must be pointed out that lack of compliance with any of these requirements renders intercepted evidence inadmissible.

Warrants for interception (or 'eavesdropping warrants')[112] are issued by a State judge. Because of the influence of the Federal Constitution and case law, non-warrant interceptions are strictly forbidden. The purpose of this requirement is to protect individuals from undue interference with their rights. This system is thought to give a more objective basis of challenge by defendants and control by the courts. Thus according to the State's Court of Appeals,

> If a warrant is required by law, the fact that the officers behaved reasonably without one is unavailing. The purpose of the warrant requirement is to interpose

[108] *People v Edelstein* (1981) 445 N.Y.S.2d 125 (CA), 126; *People v Troia* (1984) 478 N.Y.S.2d 715 (SC, App Div 2 Dept), 717; *U.S. v Ricco* (1976) 421 F.Supp 401 (S.D.N.Y) (Fed), 411.

[109] Cf. *Civil Practice Law*, art. 1311. This civil action can be initiated by the State to recover assets forming proceeds of crime.

[110] Preiser (n 666) Commentary to Art. 700.65.

[111] Cf. CPL, art. 700.65[3].

[112] An 'eavesdropping warrant' is 'the order of a justice authorizing or approving eavesdropping.' CPL, Art. 700.05[2].

> a neutral and detached Magistrate between citizens and the police to protect individuals from having to rely on the good conduct of the officer in the field for the protection of their right to be free of unreasonable searches.[113]

Warrants may only be applied for by a limited number of public and law enforcement officials. 'Applicants' can only be the State's Attorney General or a District Attorney (including the District Attorney in charge of the State's 'Organized Crime Task Force')[114] or in their absence the persons designated to act in their stead.[115] Furthermore, The Criminal Procedure Law designates the offences whose occurrence enables the respective 'applicants' to apply for an eavesdropping warrant.[116] The list is extensive. It includes many degrees of assault,[117] of possession of controlled substances,[118] eavesdropping,[119] and many forms of terrorism.[120]

An eavesdropping warrant may only be issued on ex parte application by an applicant duly authorised by State Law to prosecute the designated offence in question.[121] The warrant may not be issued for a period longer than necessary to obtain the evidence sought, but in any case no longer than 30 days,[122] which can be extended under certain circumstances.

Besides these formalities, applicants for eavesdropping warrants must: (a) show *probable cause*[123] and (b) satisfy the justice *that normal investigative procedures have been tried and failed or that it reasonable to consider their employment too dangerous or futile*.[124]

As regards *probable cause*, it is a federal constitutional requirement in the United States that 'no Warrants shall issue, but upon probable cause, supported by Oath or

---

[113] *People v Bialostok* (1993) 594 N.Y.S.2d 701 (CA), 704.

[114] This is an agency in the State of New York charged with investigating and cooperating in the prosecution of inter-County or inter-State organised crime. Cf. Executive Law, s. 70-a[1].

[115] CPL, Art. 700.05[5].

[116] CPL, Art. 700.05[8].

[117] CPL, Art. 700.05[8](b).

[118] CPL, Art. 700.05[8](c).

[119] I.e. interception can be authorised to detect unlawful interception. CPL, Art. 700.05[8](j).

[120] CPL, Art. 700.05[8](q). This section was amended in 2004 (c.1) as a response to the September 11, 2001 attacks on the World Trade Center.

[121] CPL, Art. 700.10[1].

[122] CPL, Art. 700.10[2].

[123] The applicant must prove probable cause of the past or present commission of a designated offence or that such offence is about to be committed (CPL, Art. 700.15[2]). Further, the applicant must show probable cause that 'particular communications concerning such offense will be obtained through eavesdropping' (i.e. that the interception of communications will be effective for the case at hand) (CPL, Art. 700.15[3]) and probable cause to believe that the premises whereat the interception is to be conducted are being used for the commission of the designated offence (CPL, Art. 700.15[5]).

[124] CPL, Art. 700.15.

affirmation.'[125] Probable cause may loosely be defined as the belief by a reasonable person that a crime has been or will be committed. It is thus reasonable inference based on the facts known to the issuing justice before issuing the warrant. It is to be noted that probable cause can be established with the aid of informants[126] or by the use of previously intercepted communications,[127] among many other methods.

Under New York Law, the applicant for an eavesdropping warrant must prove the same probable cause standard needed as for the search warrants of article 690 CPL.[128] This standard is that set by the Supreme Court of the United States in the cases of *Aguilar* and *Spinelli*,[129] which in short requires the issuing justice be satisfied that (i) the information supporting the assertion that an offence has been committed is reliable and (ii) that the commission of such offence can be reasonably inferred from this information.[130]

With regards to the *exhaustion and futility of normal investigative procedures*, applicant must show that other procedures have failed or cannot be used given the concrete circumstances of each case. [131] This affirmation should be supported with affidavits by experts and police officers.[132] The aim behind this requirement is not that all other investigative methods be exhausted before resorting to intercepting

---

[125] *US Constitution* (n 633) IV Amendment.

[126] Generally, however, the information supplied by informants is corroborated with other information known to the Police before issuing the warrant. E.g.: *People v DiNapoli* (SC, App Div 1 Dept) (1999) 687 N.Y.S.2d 629, 630 [highly trustworthy informant's tip corroborated by duly authorized surveillance]; *People v Giraldo* (2000) 705 N.Y.S.2d 334 (SC, App Div 1 Dept), 336 [made use of informants, members of narcotics conspiracy investigated, and telephone record analysis, all 'ampl[y] corroborating' the drug trafficking sought to be investigated by the interception of communications].

[127] *U.S. v Fury* (1977) 554 F.2d 522 (CA) (Fed), 530-531.

[128] *People v Truver* (1997) 665 N.Y.S.2d 995 (SC, App Div 4 Dept), 996.

[129] Cf. *People v Glass* (1988) 524 N.Y.S.2d 936 (SC, App Div 4th Dept), 937.

[130] *Aguilar v Texas* (1964) 378 U.S. 108 (SC) (Fed), 114; *Spinelli v U.S.* (1969) 393 US 410 (SC US) (Fed), 413; Cf. *People v Truver* (n 128) 996 ['The warrant is valid if the application demonstrates reasonable grounds to believe that a crime has been or is about to be committed and that evidence of that crime might be obtained through the use of electronic surveillance.']

[131] *U.S. v Lilla* (1983) 699 F.2d 99 (CA) (Fed), 104-105 ['Like other courts, we reject generalized and conclusory statements that other investigative procedures would prove unsuccessful.' Warrant not called for because suspect was not apprehensive to deal with undercover New York State agents already in place and there was a lack of showing the danger or unlikelihood of success of other methods]; *People v Acevedo* (1999) 692 N.Y.S.2d 11 (SC, App Div 1 Dept), 12 [informants had failed to infiltrate highly sophisticated narcotics and money-laundering operation and physical search would have been futile to convict all suspects, although some 'significant' information had been obtained by normal methods]; *People v Barber* (2000) 703 N.Y.S.2d 328 (SC, App Div 4 Dept), 329 [modus operandi of narcotics-related suspect, who, inter alia, only operated by phone, refused to deal with unknown persons and had promised violence against police officers, made the use of informants further than already used futile. Eavesdropping warrant was thus called for].

[132] Such affidavits are to be construed in a 'commonsense and realistic fashion' (*People v Truver* (n 1288) 996) and may be challenged by defendant if he proves that the affiant made knowingly (or recklessly) false statements of fact (*People v Fonville* (SC, App Div 4 Dept) (1998) 681 N.Y.S.2d 420, 423).

communications.[133] Rather, the aim of this provision is that the interception of communications not be used as the initial step in a criminal investigation[134] or as a 'useful additional tool'[135] *where other less intrusive methods are still effective to secure convictions*.

(b) Requirements to be met in the execution of the Eavesdropping Warrant

Upon satisfaction that all requirements have been met the justices may issue eavesdropping warrants. New York Law mandates eavesdropping warrants should remain in force more time than is needed to obtain the evidence sought, but never more than thirty days[136] after the date of its issuance.[137] After this, warrants may be extended[138] in some circumstances.

Pursuant to article 700.30 CPL, such warrants must basically evidence that all requirements of the application have been met. Nevertheless, at this junction there are significant differences which influence the admissibility of evidence later on.

The eavesdropping warrant must name the law enforcement agency empowered to *carry out* the interception. As opposed to the applicant, who will later be the prosecutor of the offence committed, these law enforcement agents are the ones which will conduct the actual interception. Absent this designation, no agency would have the requisite authority to intercept communications,[139] rendering inadmissible any evidence derived from their work.

Furthermore, the warrant must contain a description of the observations and type of communications sought to be obtained. This enhances the *minimisation requirement* established in the Federal Constitution for intercepted communications. As defined by New York's Supreme Court in *People v Floyd*, the minimisation requirement is

> [A] good faith and reasonable effort to keep the number of nonpertinent [sic] calls intercepted to the smallest practicable number (…) [to be determined] on a case-by-case basis with regard to the scope and circumstances of the particular investigation under review.[140]

---

[133] *People v Versace* (1980) 426 N.Y.S.2d 61 (SC, App Div 2 Dept), 64.

[134] *People v Gallina 1983* (n 966) 418; *U.S. v Feola* (1987) 651 F.Supp. 1068 (S.D.N.Y.) (Fed), 1104.

[135] *People v Brenes* (1976) 385 N.Y.S.2d 530 (SC, App Div 1 Dept), 531-532.

[136] CPL, Art. 700.10[2].

[137] *People v Paluska* (1985) 491 N.Y.S.2d 999 (SC, App Div 3 Dept), 1000.

[138] CPL, Art. Art. 700.40. This happens at any time prior to the expiration of the original warrant and upon *ex parte* application similar to that of the original warrant, but with an added statement explaining the results obtained or a reasonable explanation as to the failure to obtain them. If granted, the order of extension must fulfil all requirements set for eavesdropping warrants.

[139] CPL, Art. 700.35[1]; *People v Guercio* (1977) 394 N.Y.S.2d 536, 537.

[140] *People v Floyd* (1976) 392 N.Y.S.2d 257 (CA), 261; Cf. *Berger* (n 644) 57-60; Cf. *Scott v United States* (1978) 436 US 128 (SC) (Fed), 140-141.

Its purpose is to prevent officers from obtaining a 'roving commission' for seizing all communications.[141] Not observing this requirement offends the Fourth Amendment to the Federal Constitution and *renders inadmissible all evidence obtained through interception.*

Nevertheless, it is a reasonableness standard. New York Law is not blind to the circumstances of each case, such as the scope of the investigation undertaken,[142] the nature of the parties, among others.[143] In each case, what must be shown is a reasonable effort to keep the number of interceptions to a minimum.[144] Additionally, in order for a conversation to be determined non-pertinent, it is unavoidable that some parts of it must be overheard.[145] Therefore, contrary to most requirements under New York Law, some inobservance of the minimisation requirement will not necessarily render intercepted evidence inadmissible at trial.

Under New York Law, the minimisation requirement can only be lifted by a court order.[146] This could occur, for example, if a foreign language is employed by parties of the communication and the services of a translator are needed but cannot be procured during the interception operation.[147] This allows law enforcement agents to intercept all conversations, pertinent or not, and to have them translated later on. However this must be authorised by the issuing judge and a statement in this regard must be included on the application.

On another view, New York Law authorises law enforcement agents to disclose information obtained in the course of interception in order to amend the original terms of the warrant. Such amendment is only required when offences not within the ambit of the

---

[141] *Katz* (n 79) 59; Cf. *People v Basilicato* (1984) 485 N.Y.S.2d 7 (CA), 12-13 [warrant authorizing telephone interceptions did not empower police officers to place microphones and overhear conversations made when the telephone was 'off the hook', even if the telephone had been put thus in order to avoid interruptions by telephone callers and the content of the overheard conversations later proved key at convicting suspects].

[142] *People v Floyd* (n 1400) 252 [when conspiracy investigated is broad, surveillance may be larger than ususal, although all efforts to secure minimization of 'innocent' callas should be made]; *People v Carter* (1975) 365 N.Y.S.2d 964 (CC New York), 969 [takes account of fact that criminal conversations may appear to be innocent at the beginning and flexibility is due to the police].

[143] *People v Brenes* (1977) 396 N.Y.S.2d 629 (CA), 633 ['Necessarily, many variables enter into the determination of whether that burden has been met. Obviously, what may be a reasonable procedure and 'a conscientious effort' under the circumstances of one investigation may be unjustifiable under others. The nature and scope of an actual investigation in progress; the character and sophistication of the parties who are its targets and the nature of their expected associates; the extent of the official supervision devoted to each step of the surveillance; the possibility and practicality of determining, contemporaneously with their interception, whether particular conversations are in fact pertinent to the objectives of the investigation; these are among the many factors to be taken into account.']

[144] *People v Brenes* 1977 (n 1433) 633; *People v Estrada* (1978) 410 N.Y.S.2d 757 (SC), 759.

[145] *People v Estrada* (n 1444) 760 [this does not exempt the authorities of duty to record up to the point whereat they considered the conversation to be innocent and had the intercepting equipment turned off]; *U.S. v Hinton* (1976) 543 F.2d 1002 (CA) (Fed), 1012.

[146] *Preiser* (n 666) Commentary to Art. 700.35 CPL.

[147] CPL, Art. 700.35[4].

original warrant have been detected,[148] with a view to legalising any prosecution made on the basis of such new evidence as may be found.[149] This is what is termed the 'plain view' provision, which has been included in the constitutional requirement of description of evidence in each warrant by allowing for the retroactive amendment of warrants.[150] However, warrants need no amendment when new information represents detection of new suspects committing *the same designated offences* for which the eavesdropping warrant was issued.[151] The conversations intercepted can be used as evidence against these new suspects.

Additionally, a later admission of evidence in any criminal trial cannot be procured if law enforcement agencies do not keep the recordings of intercepted conversations under seal in a way that prevents alterations.[152] To ensure compliance with this, New York Law directs law enforcement agents to turn in all recordings to the issuing justice, so the latter seal them 'immediately.'[153] This requirement is strictly construed by Courts because in establishing a chain of custody of the evidence to be later used at trial it ensures evidential reliability.[154]

Nonetheless, 'immediate' is not construed as 'instantaneous'.[155] Rather, it represents a burden on the prosecution to offer a satisfactory explanation for any delay in sealing.[156] The reasonableness of each delay will depend on the circumstances of each case.[157]

---

[148] If it is the case that unforeseen offences fall within the type of communications sought by the warrant there is no need to amend it. Cf. *People v Wakefield Financial Corp.* (n 1066) 384 ['The 'not otherwise sought' requirement is designed to insure that the eavesdropping process not be abused to the extent that the police may utilize the process to seek evidence as to crimes other than the ones they disclose to the court in seeking the warrant. To the extent that the crime discovered is within the ambit of the crimes disclosed to the judicial officer approving the warrant, the requirement of the statute is satisfied.']; Cf. *People v Cicero* (1983) 468 N.Y.S.2d 798 (SC), 800 [conversations 'obviously pertained to designated offenses', thus no amendment to original warrant needed].

[149] *People v Ruffino* (1970) 309 N.Y.S.2d 805 (SC), 812; *People v Rizzo* (1972) 333 N.Y.S.2d 152 (SC), 166.

[150] Preiser (n 666) Commentary to Art. 700.65 CPL; It is to be noted that police officers can correctly listen to the whole of the new incriminating conversation before applying for amendment to warrant without offending minimisation requirements. Cf. *People v Calogero* (1980) 429 N.Y.S.2d 970 (SC, App Div 4 Dept), 974-975.

[151] *People v Huff* (1972) 335 N.Y.S.2d 118 (CC Onondaga), 121; *People v Casalini* (1984) 483 N.Y.S.2d 899 (SC), 901-902.

[152] CPL, Art. 700.35[3].

[153] CPL, Art. 700.50[2].

[154] *People v Basilicato* (1984) 485 N.Y.S.2d 7 (CA), 13; *People v Fonville* (n 132) 426; Cf. *U.S. v Ricco* (n 1088), 410-411.

[155] *People v Scaccia* (1974) 390 N.Y.S.2d 743 (SC, App Div 4 Dept), 745; *U.S. v Ricco* (n 1088) 410.

[156] *People v Basilicato* (n 1544) 13 [because of the 'potential for (…) abuse' implied].

[157] *People v Scaccia* (n 1555) 745. Cf. *People v Winograd* (1986) 509 N.Y.S.2d 512 (CA), 519 [weekend between expiration of warrant and sealing not a satisfactory explanation of delay].

As stated previously, the lack of compliance with this requirement allows for suppression of all relevant evidence without the need for the suspect to show prejudice or even tampering with the evidence.[158]

Finally, New York Law imposes on law enforcement agents:

- An obligation to report to the issuing justice the progress of the interception operation if the warrant so orders.[159] It is optional for the issuing judge to establish this reporting requirement,[160] although Courts have expressed strong preference for eavesdropping warrants to be issued with progress report requirements, especially in cases where the investigation is intense and/or prolonged.[161] If inserted in the warrant, however, the lack of compliance with the progress report requirement makes inadmissible all evidence collected after this report was due.[162]
- An obligation to notify to the person named in the warrant or such persons as the issuing justice (after all eavesdropping warrants have expired) deems should be notified of the fact of the interception. This notification must be carried out within a reasonable time -but never more than ninety days- after the warrants in question have expired and in the manner prescribed by the issuing justice.[163] A federal requirement,[164] the purpose of such notification is to let those whose phones have been intercepted to seek civil redress should they deem their privacy has been unlawfully invaded[165] and as a way to let such persons that may not be embroiled in a criminal action know they have been the subject of investigation.[166] However, the defendant needs to show prejudice in order to have evidence suppressed if the fact the interceptions have taken place has not been informed to him/her.[167] Moreover, no duty to inform exists if the law enforcement agents can show the issuing justice that 'exigent circumstances' should preclude notification from happening.[168]

---

[158] *People v Winograd* (n 1577) 518.

[159] CPL, Art. 700.50[1].

[160] *People v Floyd* (n 1400) 264.

[161] *People v Castania* (1973) 340 N.Y.S.2d 829 (CC Monroe), 832; *People v Floyd* (n 1400) 264.

[162] *People v Cantineri* (1987) 521 N.Y.S.2d 914 (SC, App Div 4 Dept), 915.

[163] CPL, Art. 700.50[3].

[164] 18 USC § 2518[8(d)].

[165] This is a possibility under Federal Law. 18 USC § 2520.

[166] *U.S. v Donovan* (1977) 429 US 413 (SC US) (Fed), 428-432; Cf. *Preiser* (n 666) Commentary to art. 700.50 CPL.

[167] *People v DiLorenzo* (1971) 330 N.Y.S.2d 720 (CC Rockland), 728.

[168] CPL, Art. 700.50[4]. Regarding interception, New York Law (CPL, Art. 700.05[7]) defines 'exigent circumstances' as 'conditions requiring the preservation of secrecy, and whereby there is a reasonable likelihood that a continuing investigation would be thwarted by alerting any of the persons subject to surveillance to the fact that such surveillance had occurred.'

C. The Relevance of the New York Experience to the UK

Contrary to the position of English Law, New York Law mandates full disclosure of the contents of all intercepted communications to criminal defendants. This has resulted in no small measure from the way the Federal Constitution, legislation and case law conceive an interception of communications: an intrusion into constitutionally protected areas of privacy and security of the person. As seen previously, this conception is not alien to the European Convention and human rights legislation in English Law.

Perhaps more interesting is the situation of the New York Law defendant when compared with his English counterpart. Defendants are allowed to question the way every action has been carried out, ranging from the omission of formalities to whether the amount of non-pertinent conversations intercepted was excessive. This ability to question the legality of interceptions is virtually limitless. Contrary to English Law, the fact that an offence might have been committed by any law enforcement agent or prosecutor in pursuance of their duties does not debar defendants from asserting their perceived rights. And thus it may be said that the defendant and the prosecutor are placed on a more equal footing than is the case in English Law.

In this regard, the idea that a Minister or a police officer may issue warrants at their discretion is alien to this system, which requires the authorisation of a judge for every case. This judge has an active role in the execution, renewal or extension of the eavesdropping warrant and in establishing a chain of custody which emphasises the reliability of intercept evidence. Prosecutors and law enforcement agents have to comply with all requirements laid down by New York Law at every stage of the process. Significantly, the burden of proving the propriety of the interception of communications, and thus the admissibility of evidence, rests on their shoulders.

In general, New York Law is stricter in demanding compliance with issuing requirements: those at the earlier stages of the interception operation. Interception undertaken despite an omission of these requirements will result in inadmissibility of evidence. The same could be said of those provisions tending to establish an appropriate chain of custody. By contrast, whilst the operation is being executed, the standards seem to become more of reasonableness than black-letter-law-compliance. Indeed, in New York, as put by the Court of Appeals, ‘‘Strict compliance’ does not entail hypertechnical or strained obedience, nor is common sense its enemy.’[169]

Hence New York Law could become an important example to follow for the United Kingdom. It protects the defendant to the strictest degree possible, without stifling its law enforcement agents. The disclosure of the contents of evidence to the defendant or even to persons not tried after the intercepted communications are recorded does not seem to detract from the State’s ability to effectively prosecute criminal offenders by means of intercepted communications. The State makes frequent use of these means to prosecute sophisticated crime rings and large scale illegal operations regardless of the disclosure requirement. The many fears held in this regard by English Law may well prove to be unfounded.

[169] Darling (n 96) 87.

II. The Admissibility of Intercept Evidence in Canada

A. Canadian Legislation

The admissibility of intercept evidence in criminal proceedings in Canada is dependent upon whether the manner in which such evidence obtained is in accordance with the legal bounds set out in the *Canadian Criminal Code*.[170] The provisions in Part VI of the *Criminal Code* under the heading 'Invasion of Privacy' make it an offence to intercept a private communication unless the interception is carried out under two circumstances:

- it is intercepted by someone who has the consent of either the originator or the person intended by the originator to receive the communication; or
- it is intercepted in accordance with a prior authorization.[171]

In these two cases interception is lawful and the evidence obtained will be admissible. A closer examination of this aspect of the legislation where the legality of obtainment affects the admissibility of intercepted private communication is given below, with an emphasis on the latter circumstance of prior authorization (the issue of consent will be returned to below).

The legislation is only concerned with the interception by 'electro-magnetic, acoustic, mechanical or other device' of a 'private communication'.[172] 'Private communications' are defined broadly in s. 183 as:

> any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it.

The interception of private communications covers telephone wiretaps and video surveillance (but not those without soundtrack) according to the definition of telecommunication in s. 28 of the *Interpretation Act*.[173] However, the extent to which it covers access to e-mail or other internet-based communications is unclear (which at present is still the topic of much legal debate),[174] since such communications are usually

---

[170] HJ Cox, *Criminal Evidence Handbook* (2nd edn Canada Law Book Inc., Aurora 1991) 216; J Sopinka, SN Lederman and AW Bryant, *The Law of Evidence in Canada* (2nd edn Butterworths, Toronto 1999) 462.

[171] AW Mewett and S Nakatsuru, *An Introduction to the Criminal Process in Canada* (4th edn Carswell, Toronto 2000) 51.

[172] RJ Delisle and D Stuart, *Learning Canadian Criminal Procedure* (4th edn Carswell, Scarborough 1996) 179; J Sopinka, SN Lederman and AW Bryant (n 170) 462.

[173] HJ Cox, (n 170) 207; D Watt, *Law of Electronic Surveillance in Canada* (Carswell, Toronto 1979) 27.

[174] RJ Daniels, P Macklem and K Roach (eds), *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (University of Toronto Press, Toronto 2001); D Valiquet, 'Telecommunications and Lawful Access: The Legislative Situation in Canada' Parliament Information and Research Service. Electronic version: *http://www.parl.gc.ca/information/library/PRBpubs/prb0565-e.html* (2006).

accessed not in real time, but rather from a computer where they have been stored (in which case access to them could be considered a 'search' rather than an 'interception').[175]

Law enforcement officials are permitted to intercept or monitor private communications (often referred to as 'wiretap') only under strict rules set out in the *Criminal Code*. With respect to the issue of authorization, where one party to the communication consents to the interception, the law enforcement agency seeking authorization to intercept must satisfy a judge that there are reasonable grounds to believe that an offence has been or will be committed, and that relevant information is likely to be collected via the interception. Where no party to the communication has consented, the law enforcement agency must demonstrate to the judge that other less intrusive investigatory means have been tried and failed or that the urgency of the matter makes other procedures impractical, and that the interception is in the best interests of justice. For certain specific offences such as terrorism, the judge issuing the authorization need only be satisfied that the authorization is in the best interests of the administration of justice.[176]

Interception authorizations generally last for no more than 60 days. However, judges may authorize 'emergency authorizations' without any particular 'reasonable grounds' or other test; these have a 36 hour maximum duration. In addition, interceptions can be carried out without judicial authorization in the following situations:[177]

- where one party consents, and the law enforcement agency reasonably believe that bodily harm may occur to the person consenting, and the interception is meant to prevent bodily harm (s. 184.1);
- where the law enforcement agency reasonably believes that the urgency of the situation is such that authorization is impossible and that interception is immediately necessary to prevent an unlawful act that would cause serious harm to person or property, and that a party to the communication is the perpetrator or victim (s. 184.4); and
- by the Canadian Security Establishment (CSE) for the purpose of obtaining foreign intelligence or for the protection of the government's computer systems

[175] As stated in s. 28 of the Interpretation Act (Watt (n 173) 27), the definition of 'telecommunication' is 'Any transmission, emission or reception of signs, signals, writing, images or sounds or intelligence of any nature by wire, radio, visual or other electromagnetic system.' It is to be noted here that the definition of 'interception of private communication' in the Canadian context differs from that of the definition of 'interception and transmission' in the United Kingdom Law. Under s. 2(2) and (4) of the Regulation of Investigatory Powers Act 2000 (RIPA) in the United Kingdom, interception means the: modification of or interference with a telecommunications system; monitoring of transmissions made by such a system by means of the system itself or through wireless telegraphy or other apparatus; the interception of a postal item. Therefore, surveillance activities are not included in the legal definition of interception of communications in the United Kingdom, while in Canada the legislation is not concerned with the interception of postal items.

[176] CIPPIC 'Lawful Access: Police Surveillance.' Electronic Version: *http://www.cippic.ca/en/faqs-resources/lawful-access/* (2006); CT Griffith and SN Verdun-Jones, *Canadian Criminal Justice* (2nd edn Harcourt Brace, Toronto 1994) 134.

[177] Ibid.

and networks, where authorized by the Minister of National Defence. CSE intercepts for the purpose of collecting foreign intelligence must be directed at foreign entities located outside Canada (s. 273.65, *Anti-Terrorism Act*).

B. Admissibility of Intercept Evidence under the Criminal Code

Many cases involving interception of private communication have contributed to major amendments in legislation as well as court procedures and decisions with regard to the admissibility of intercepted private communications provisions of the Criminal Code.[178] Such enactment of major changes were in response to concerns expressed by police and prosecutors that various Charter of Rights decisions, striking down several powers to use electronic surveillance, had left police without the necessary power and had put police officers and informers at risk. Selected below are the cases which prompted these amendments. The particular issues examined are the legality of interception, issue of consent, procedure for establishing illegality, and access to 'sealed packet'.

i. Legality of Interception

Except for the two situations mentioned in A.i, the *Criminal Code* had previously made any illegal interception of private communications automatically inadmissible as evidence in trial. However, the parliament repealed this provision. Consequently, the admissibility of any such illegally obtained evidence would be determined under s. 8 and 24(2) of the *Charter of Rights*. Any illegal intercept private communication obtained as a result of the illegal interception would be excluded where its admissions would bring the administration of justice into disrepute.[179] An example of evidence obtained derivatively from an illegal intercept is, if, as a result, the police locate a cache of drugs, the evidence of the drugs themselves would only be inadmissible if its admission would bring the administration of justice into disrepute. Thus, if the interception is unlawful (that is, not made under a valid authorization or with the consent of one of the parties), the evidence of the communication *maybe* inadmissible as evidence at trial, depending on the 'disrepute test'.[180]

It should be noted that some communications, even if lawfully intercepted, are not admissible if they involve a 'privileged communication'.[181] The two most commonly encountered in this context are a communication between a lawyer and client and a communication between a husband and wife. Usually, an authorization cannot be obtained to intercept communications in a lawyer's office or residence unless it is reasonable to believe that the lawyer himself (or an employee or member of his household) is a party to the offence in question. However, interception may be made at the client's house and involve a conversation he has with his lawyer or his wife. In such a

[178] JA Fontana, *The Law of Search and Seizure in Canada* (3rd edn Butterworths, Toronto 1992) ch 15.

[179] CT Griffith and SN Verdun-Jones (n 176) 137.

[180] AW Mewett and S Nakatsuru (n 171) 53.

[181] Ibid 54.

case, the conversation remains privileged and inadmissible unless the client or the wife waives the privilege and consents to its admission.[182]

ii. The Issue of Consent

While the *Criminal Code* provides for consent interceptions to be legal, in the case of *R. v Duarte*,[183] the Supreme Court added another dimension to the problem. There, during a drug-trafficking investigation, the police installed an audio-visual recorder in an apartment occupied by an informer. The undercover police officer and the informant consented to interceptions pursuant to s. 184(2)(a) [formerly s. 178.11(2)(a)] of the *Criminal Code*. The accused later discussed a cocaine transaction with the undercover officer and the informer at the apartment. Charged with the offence of conspiracy to import a narcotic, the accused challenged the validity of s. 184(2)(a), which excepts the interception of conversations to which one of the parties consents from the prohibition of unauthorized electronic surveillance. The Supreme Court of Canada held that, in the absence of judicial authorization, 'participant' interceptions by an agent of the state pursuant to s. 184(2)(a) constituted an unreasonable search and seizure contrary to s. 8 of the *Charter of Rights*, which violated the rights of the accused. Thus, the evidence was inadmissible since its admission would bring the administration of justice into disrepute.[184]

Following the decision in *Duarte*, the *Criminal Code* was amended to allow for judicially authorized consent interceptions of private communications under the circumstances in which *Duarte* took place. The *Criminal Code* was further amended to permit a private communication to be intercepted without a judicial authorization by an agent of the state, provided either the originator or the person intended to receive the private communication consents and the agent of the state believes on reasonable and probable grounds that there is danger of bodily harm to the person who consented to the interception. The evidential use of the contents of the intercepted private communication is restricted to proceedings in which actual, attempted, or threatened bodily harm is alleged or to obtain a search warrant, a warrant of arrest, or an authorization under Part VI of the *Criminal Code*.[185]

iii. Procedure for Establishing Admissibility

The procedural mosaic to determine admissibility of intercepted private communication was set out in *R. v Garofoli*.[186] The Supreme Court of Canada in *Garofoli* reiterated that the issuing judge must be satisfied that there are reasonable and probable grounds to believe that an offence has been or is being committed and that the authorization sought,

[182] Ibid.

[183] [1990] 1 SCR 30 (SC).

[184] Delisle and Stuart (n 172) 183; JA Fontana (n 178) 653; Mewett and Nakatsuru (n 180) 53; Sopinka, Lederman and Bryant (n 170) 463.

[185] Sopinka, Lederman and Bryant ibid.

[186] [1990] 2 SCR 1421 (SC).

will afford evidence of that offence. The procedures available for challenging an authorization are:[187]

- a 'Parsons voir dire' (named after *R. v Parsons*[188]), a hearing before the trial judge to determine whether the authorization is valid on its face, whether the police executed the interception within the terms of the authorization, and whether statutory requirements such as reasonable notice were complied with;
- a 'Wilson application' (named after *Wilson v R.*[189]), a hearing before the issuing court, to determine the substantive or subfacial validity of the affidavit, the remedy here being the setting aside of the authorization;
- a 'Garofoli hearing' (named after *R. v Garofoli*), a hearing before the trial judge to determine whether the authorization complies with s. 8 of the Charter of Rights, the remedy here being whether or not the evidence should be excluded under s. 24(2);
- a 'Vanweenan hearing' (named after one of the appellants in *R. v Chesson*[190]), a hearing before the trial judge to determine whether the authorization names all the known persons as required by ss. 178.12(1)(e) and 178.13 (2) or the Criminal Code, the remedy being exclusion of the evidence.

iv. Access to Sealed Packet

The Ontario Court of Appeal in *R. v Playford*[191] ruled that where an accused at trial wishes to challenge a judicial authorization to intercept private communications on the basis that it should not have been issued, he is entitled to have access to the 'sealed packet' containing the affidavit, which was used on the application.[192] This is subject to applying the procedures necessary to protect the identity of police informants. There is no requirement, according to the court, that the accused must first make out a *prima facie* case of fraud, non-disclosure, or misleading disclosure. The court says that once the investigation has been completed and an accused is charged, there is no logical or policy reason to refuse to reveal the contents of the sealed packet subject to proper editing. As Goodman states (1988):[193]

> In my opinion, it must be emphasized that the provisions of s. 178.14(1) [now s. 187(1)] do not indicate that Parliament intended that the contents of the packet should be kept secret forever. It gave to the judges designated in s. 178.14(1)(a)(ii), the right to order that the packet may be opened or the contents removed. Such orders call for the judicial

[187] Fontana (n 178) 654; Sopinka, Lederman and Bryant (n 170) 464.

[188] (1977) 37 CCC (2d) 497 (Ont CA).

[189] [1983] 2 SCR 594 (SC).

[190] [1988] 2 SCR 148 (SC).

[191] (1987), 40 CCC (3d) 142 (Ont CA).

[192] Fontana (n 178) 654.

[193] Ibid.

> exercise of discretion. As previously indicated it would be extremely difficult to justify a refusal by a judge to order the opening of a packet and the production of the contents where such order would not interfere with the investigation of a crime and the alleged perpetration thereof and where, if necessary, appropriate safeguards are taken to protect informers, undercover agents and secret police methods.

In *Dersch v Canada*,[194] Dickson held that an accused, who seeks access to the documents relating to the application for a wire-tap authorization is not required to show *prima facie* misconduct.[195] The assertion that the admission of the evidence is challenged and that access is required in order to allow full answer and defence is adequate. The decision in *Dersch* was referred to again by the Supreme Court of Canada in *R. v Lachance*,[196] where that principle was reiterated. In *R. v Garofoli*, the Supreme Court of Canada again held that the appellate court below was right to open the sealed packets since the accused is entitled, subject to editing, to have the contents produced in order to have him make full answer and defence.[197]

As well, in *R. v Zito*,[198] the Crown's drug trafficking case depended in part on evidence of communications intercepted pursuant to an authorization. However, at trial, the accused had been denied access to the affidavits on which the authorization had been granted. The Supreme Court of Canada, following the decision in *Dersch*, agreed with the Court of Appeal's decision to grant the accused a new trial. Based on *Garofoli*, the opening of the sealed packet is within the discretion of the judge hearing the application for access. Thus, a balancing of the interests between the accused and the public, in the absence of special concerns, would result in the granting of access.[199]

C. The Relevance of the Canadian Experience to the UK

In relation to the concerns of admitting intercept evidence at court in the United Kingdom as shown above, the issue of access to the sealed packet in the Canadian courts as described in section 3.4 seems to coincide most closely with these concerns. As mentioned previously, although an accused may apply to the trial judge to unseal the 'packet' containing the documents for the purpose of allowing the accused to review the documents for trial preparation, the judge has the discretion in granting or refusing such an application. In case that access is granted, the judge, then, shall not provide the accused with a copy of the document until the Crown has an opportunity to delete any part of the document. Even then, where the accused receives an edited document, he or she may make a further application to the trial judge to order that any part of the deleted portions of the document be furnished to him or her in order to make full answer and defence.

---

[194] [1990] 2 SCR 1505 (SC).

[195] Fontana (n 178) 654.

[196] [1990] 2 SCR 000 (SC).

[197] Fontana (n 178) 654.

[198] [1990] 2 SCR 000 (SC).

[199] Fontana (n 178) 654.

The reasons for the power of discretion given to the judge and the Crown under such circumstances are: ensure a balance of interest for both the accused and the public, and; ensure any other special interests are protected. In view of these reasons, it can be reiterated what Goodman stated in view of such circumstances: 'If necessary, appropriate safeguards are taken to protect informers, undercover agents and secret police methods.' [200]

Thus, by comparison to past issues and difficulties encountered by Canadian courts, it does appear that the United Kingdom's concerns over the potential exposure of interception technology and methods, informant and police identity, and any other intelligence and information in the court process are valid. However, the Canadian situation shows that if proper amendments in the criminal procedure can be made these concerns can be addressed. In particular, the Canadian context is informative in demonstrating how the United Kingdom can protect the interests of those involved by incorporating the power of discretion at the particular stage of 'application for access to sealed packet' in the judicial process.

[200] Ibid 653.

III. The Admissibility of Intercept Evidence in South Africa

A. South African Legislation

The South African Constitution recognises the right to privacy in South Africa as a fundamental right that includes the right not to have the privacy of one's communications infringed (Section 14 of the South African Constitution of 1996). The Regulation of Interception of Communications and Provision of Communication-related Act, however, limits the right to privacy in certain circumstances. The Act provides for judicial oversight in granting interception directions and allows for interception evidence to be admitted in criminal proceedings (subject to the Prevention of Organised Crime Act 1998). This piece therefore seeks to address the measures South Africa has undertaken to achieve a balance between the right to privacy and the right to security—as underlined in South Africa's Constitution of 1996—when dealing with the issue of intercept evidence.

i. South African Constitution and International Agreements

Responding to the gross interferences with peoples' right to privacy during the apartheid era in South Africa, the South African Constitution of 1996 states that everyone has the right to privacy which includes the right not to have their person, home or property searched, their possessions seized or the privacy of their communications infringed (Section 14). However, everyone has the right of access to any information held by the state and any information that is held by another person as required for the exercise or protection of any rights (Section 32(1)). Hence, national legislation ought to be enacted to give effect to this right and may provide for reasonable measures to alleviate the administrative and financial burden on the state (Section 32(2)).

The provisions of the Constitution have also been examined by the South African Constitutional Court, which delivered several judgments on the right to privacy relating to the possession of indecent or obscene photographs[201] and child pornography,[202] searches and seizures,[203] and the criminalisation of prostitution[204]. The court's interpretation of the right to privacy—based on US and European jurisprudence—emphasises the value of human dignity as the root of the right and seeks to protect an expectation of privacy that society recognises as reasonable.[205]

Apart from the constitutional provisions, international agreements entered into by South Africa are also relevant to this area of law. Of particular importance is the Council of Europe Convention on Cybercrime,[206] dealing with infringements of copyright,

[201] *Case v Minister of Safety and Security* 1996 (3) SA 617 (CC).

[202] *De Reuck v Director of Public Prosecutions (Witwatersrand Local Division)* 2004 (1) SA 406 (CC).

[203] *Bernstein v Bester* NO 1996 (2) SA 751 (CC); *Mistry v Interim National Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC).

[204] *S v Jordan* 2002 (6) SA 642 (CC).

[205] Ibid [81]; Privacy International, www.privacyinternational.org/article.shtml?cmd[347]=x-347-83780.

[206] Convention on Cybercrime of 2001, ETS 185. South Africa is one of four non-member signatories to the Convention. Other non-member signatories include the United States, Canada and Japan.

computer related fraud, child pornography and violations of network security, which had a further impact on the law reform process in South Africa.[207]

ii. Interception and Monitoring Prohibition Act

South African surveillance law was significantly amended in 1992 to increase individual privacy protections. The Interception and Monitoring Prohibition Act (No. 127 of 1992) focused primarily on telephonic and postal communications. In 1998, the South African Law Commission (SALC) began a project (SALC, Project 105, November 1998) to review existing 1992 law on the monitoring and interception of communication for crime investigation and intelligence gathering purposes, and to extend its scope to all communications networks.[208]

iii. Regulation of Interception of Communications Act

The Regulation of Interception of Communications and Provision of Communication-related Act (RICA) came into effect on 22 January 2003 (and amended in May 2006) following a series of unauthorised surveillance incidents in the late 1990s.[209] These incidents involved the monitoring of thousands of international and domestic phone calls without warrant by the South African Police Service in 1996,[210] the announcement of the opposition Democratic party that it had found surveillance devices at its parliamentary offices and national headquarters in 1999[211] and a government apology to the German government after a report that an intelligence operative had placed spy cameras outside the German embassy. [212]

RICA establishes a balance between both rights to privacy and security by providing judicial oversight and limiting interception of communication:

- under interception direction;
- by party to communication;
- with consent of party to communication;
- to prevent serious bodily harm;
- for purposes of determining location in case of emergency; or
- authorised by certain other Acts (Chapter 2).

---

[207] T Cohen, ISPA ADVISORY 10: The Regulation of Interception of Communications and Provisions of Communication-related Information Act, No. 70 of 2002, February 2003.

[208] Ibid.

[209] RICA was published in the Government Gazette of South Africa number 28075 and amended in May 2006 by the Regulation of Interception of Communications and Provision of Communication-Related Information Amendment Bill published in Government Gazette No. 28807. http://www.info.gov.za/gazette/acts/2002/a70-02.pdf and http://www.info.gov.za/gazette/bills/2006/b9-06.pdf

[210] 'Newspaper Uncovers 'Unlawful Tapping by Intelligence Units,' The Star, 21 February, 1996.

[211] 'Democratic Party Outraged by Bugging of Its Offices', Africa News, November 23, 1999.

[212] 'South Africa Admits to Spying on German Embassy', Reuters, February 6, 2000.

The Act also permits the interception of indirect communication in connection with the carrying on of business; monitoring of signal for purposes of installation or maintenance of equipment, facilities or devices; and monitoring of signal and radio frequency spectrum for purposes of managing radio frequency spectrum (Chapter 2).[213]

RICA states that no person—who is not a party to the communication, does not have prior written consent or is not acting in the course of business—may intentionally intercept, attempt to intercept, authorise or procure any other person to intercept or attempt to intercept at any place in the Republic any communication in the course of its occurrence or transmission (Sections 2, 4, 5). However, any authorised person who executes an interception direction or assists with the execution thereof may intercept any communication (Section 3). Further, a postal service provider to whom an interception direction is addressed may intercept any indirect communication, to which that interception direction relates (Section 3). Under RICA Chapter 3, an applicant may apply—orally or in writing—to a designated judge for the issuing of an interception direction (Sections 16, 17 and 23).

RICA also stipulates that the use of intercept evidence in criminal proceedings does not require exceptional measures. Section 47 states that information regarding the commission of any criminal offence, obtained by means of an interception or the provision of any real-time or archived communication-related information, under RICA or any similar Act in another country, may be admissible as evidence in criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act.[214] Accordingly, interception lawfully obtained under RICA Chapters 2 and 3 may be admissible as evidence in criminal proceedings. However, if a direction is issued by a designated judge (section 23(3)) or an oral direction is cancelled, the contents of any communication intercepted under that direction or oral direction will be inadmissible as evidence in any criminal proceedings or civil proceedings (as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act) unless the court decides that the admission of such evidence would not render the trial unfair or otherwise detrimental to the administration of justice (section 25(5)).

Finally, section 42 of RICA states that no person may disclose any information which he or she obtained in the exercising of his or her powers or the performance of his or her duties in terms of this Act *except* to any competent authority which requires it for the institution, or an investigation with a view to the institution, of any criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act.

iv. The Promotion of Access to Information Act

The Promotion of Access to Information Act (PAIA) came into effect in 2001. This Act includes a constitutional right of access to information held by the state and private

[213] Cohen (n 207).

[214] Prevention of Organised Crime Act, http://www.info.gov.za/gazette/acts/1998/a121-98.pdf#search=%22%E2%80%A2%09Prevention%20of%20Organised%20Crime%20Act%201998%22

organisations.[215] The PAIA's enforcement mechanism is left to the South African judiciary, whose role has been questioned as a result of the judges' lack of formal training in interpreting the PAIA. South Africa's Human Rights Commission has limited powers to enforce the PAIA by monitoring the use of the Act, publicising the rights that it creates, assisting the public to make requests, conducting research and publishing explanatory material about the Act.[216]

B. The Relevance of the South African Experience to the UK

The right to privacy of communications is recognised as a fundamental right under section 14 of South Africa's Constitution. However, it is universally accepted that no right is absolute in operation where reasonable grounds exist to limit that right.[217] Accordingly, the UK can draw from the South African Experience on three accounts.

First, RICA specifies the instances during which intercept evidence can be obtained. Unless party to the communication, has prior written consent or is acting in the course of business, no person is allowed to intercept or attempt to intercept communications (Sections 2, 4, 5). However, any authorised person who executes an interception direction or assists with the execution thereof may intercept any communication (Section 3).

Secondly, RICA specifies that an applicant may apply—orally or in writing—to a designated judge for the issuing of an interception direction (Sections 16, 17 and 23). As such, RICA guarantees judicial approval for the issuance of an interception direction.

Finally, the admissibility of intercept evidence under RICA does not weaken law enforcement efforts. Instead, the Act allows for intercepted communications to be used as an evidential tool rather than merely as an intelligence-gathering method. RICA stipulates that information regarding the commission of any criminal offence, obtained by means of an interception under RICA or a similar Act of another country may be admissible as evidence in criminal or civil proceedings (subject to Chapter 5 or 6 of the Prevention of Organised Crime Act). If a direction was issued by a designated judge or an oral direction was cancelled, the communication intercepted would be inadmissible unless the court decides that the admission of such evidence would not render the trial unfair or otherwise detrimental to the administration of justice (section 25(5)).

Accordingly, RICA provides for the limitation of the right to privacy in certain circumstances. Given the current crime rates in South Africa and the criminal uses to which certain telecommunications equipment is being put, a law of this nature will likely

---

[215] 'Concerns Raised over Access to Information Act,' Mail & Guardian, May 10, 2001 and Privacy International, www.privacyinternational.org/article.shtml?cmd[347]=x-347-83780 and PAIA, http://www.info.gov.za/gazette/acts/2000/a2-00.pdf#search=%22%E2%80%A2%09Promotion%20of%20Access%20to%20Information%20Act%22 and http://www.info.gov.za/gazette/acts/2002/a54-02.pdf#search=%22%E2%80%A2%09Promotion%20of%20Access%20to%20Information%20Act%22

[216] Privacy International, www.privacyinternational.org/article.shtml?cmd[347]=x-347-83780

[217] Cohen (n 207).

withstand constitutional scrutiny despite its limitations on the right to privacy.[218] Accordingly, the UK ought to consider admitting intercept evidence in court on a limited basis as prescribed under RICA.

[218] Ibid.

IV. The Admissibility of Intercept Evidence in Israel

A. Current Israeli Legislation

i. The Wiretapping Act

In Israel, the issue of intercept evidence is regulated specifically by the Wiretapping Act 1978.[219] This act was updated several times since, and most recently on March 24, 2005.

This act covers most types of intercept evidence. Under the definition of 'conversation' in §1, it is stated that a conversation can be 'in speech or in flash[220], including telephone, wireless phone, radio mobile, walkie-talkie, fax, telex, teleprinter or a communication between computers'.[221] The content of the conversation is also defined in §1, under the definition of 'in flash', and can be 'signs, signals, writing, visual forms, voices or data, that are transferred through wire, wireless, optical system, or any other electro magnetic system'.[222] However, this act does not apply to information that is already stored in a computer in which a lawful search is performed (e.g. saved email messages).[223] Henceforth, I will use 'intercept evidence' to refer to any evidence to which this act applies.

ii. The Evidence Law

In addition, and similar to the UK[224], the Israeli Evidence Law contains general privileges to protect the state security and the public interest.[225] According to these privileges, the disclosure of evidence that might harm the state security or the public interest would be excluded.

The state security privilege is defined in §44(A) in the Evidence Act 1971:

> A person does not have to give, and a court will not admit, evidence if the prime minister or the security minister expressed his/her opinion, in a decree signed by him/her, that giving this evidence might harm the state security, or if the prime minister or the security minister expressed his/her opinion, in a decree signed by him/her, that giving that evidence might harm the foreign relationships of the state, unless if a Supreme Court judge found, in an application from the litigant who seeks the disclosure of this evidence, that the need to disclose the evidence to do justice overweighs the interest exists not to disclose it.

The public interest privilege is defined in §45 to the Evidence Act 1971:

---

[219] Unfortunately, there is no official Israeli translation to English. Hence, the translation in this report is mine, with a conscious effort to preserve the literal meaning.

[220] See below for the definition of 'in flash'.

[221] §1 'Definitions', under the term of 'Conversation'.

[222] §1 'Definitions', under the term 'In flash'.

[223] §23A to the Criminal Legal Procedure Act 1969, added on 1995 by the Computers Act 1995, §11.

[224] For details about the British jurisprudence around the public interest privilege, P Roberts and A Zuckerman, *Criminal Evidence* (OUP, Oxford 2004) 238-244.

[225] §44 and §45 correspondently, the Evidence Act 1971.

> A person does not have to give, and a court will not admit, evidence if a minister expressed his/her opinion, in a decree signed by him/her, that giving that evidence might harm an important public matter, unless if the court discussing the case found, in an application from the litigant who seeks the disclosure of this evidence, that the need to disclose the evidence to do justice overweighs the interest exists not to disclose it.

The privileges differ in several procedural matters.[226] However, the test in both privileges is the same: whether 'the need to disclose the evidence to do justice overweighs the interest exists not to disclose it.'

B. Admissibility of Intercept Evidence under both Acts

i. Evidence Required for the Prosecution Case

From the first version of the Wiretapping Act, almost thirty years ago, legally-obtained intercept evidence was considered admissible for criminal proceedings. §13(C) states 'Intercept evidence that was legally-obtained will not be admissible in any proceedings that is not a criminal proceeding managed by the state'.[227] To clarify this further, §13(C1) was added: 'Intercept evidence that was legally-obtained will be admissible as evidence in criminal proceedings to prove any criminal offence.'

Most of the scholarly and judiciary debate in this subject focuses on the admissibility of *illegally*-obtained intercept evidence.[228] In contrast, the issue of the admissibility of legally-obtained evidence is not controversial. The statutory situation is clear so there is no case law in this question. As for the scholarly literature, I could not find any debate around this issue.[229]

ii. Evidence Required for the Defence Case

The question that arises regarding these privileges is whether to refuse the privilege request when the evidence is required for the defence of the accused. This question was directly discussed in the *Livni* case[230]. In this case, a group of Israeli Jews were accused in terrorist activity against Arabs. Agreeing to the request of the Security Service, the security minister issued a privilege decree to exclude all evidence regarding the personal details of the Security Service investigators, their working methods, the information they held and the ways in which it was achieved.

---

[226] For example, the minister who is entitled to request the privilege (prime minister and security minister only in §44(A) in comparison to any minister in §45), or the judicial panel that can approve its disclosure (a Supreme Court judge in §44(A) in comparison to the panel discussing the case in §45).

[227] In rare occasions, criminal proceedings in Israel can be managed by an individual.

[228] Until very recently, there was no overarching exclusion rule for illegally obtained evidence in Israel. However, in a recent verdict given on 4.5.2006, the Israeli Supreme Court adopted the exclusionary doctrine for illegally obtained evidence. 5121/98 *Issascharov v General Martial Attorney* (CA) (In Hebrew).

[229] However, there is a potentially relevant article (accessible only in hard copy in Israel), N Zaltsman, 'Wiring Tape as a Document and the Evidential Requirement for Writing' (1987) 12 Iyunei Mishpat 77.

[230] 838/84 *Menahem Livny and others v The State of Israel* (BS).

Justice Aharon Barak (nowadays the president of the Israeli Supreme Court) determined that whenever the evidence is essential for the defence, the privilege request should be refused regardless the risk to the state security because no interest is more important than the prevention of an erroneous conviction of the innocent:

> If the investigation material, to which the privilege applies, is essential to the defence of the accused, then, of course, the justice requires its disclosure, and this consideration overweighs any possible security consideration. No security argument, even the most worthy, does not weigh more, in the relative weights of a given criminal proceedings, than the weight of conviction of an innocent. It is preferable to acquit an accused that his/her guilt cannot be proved because the need to disclose evidence that there is a security interest not to disclose it, over the conviction of an accused that his/her innocence cannot be proved because of the need to not disclose a privileged evidence.[231]

Moreover, the essentiality test is unaffected by the gravity of the charges. Justice Barak clearly states that 'For that matter, I see no importance in the type of the offence with which the accused is charged, and to the punishment that is expected to him/her. Convicting an innocent is such a deep and painful impact on the procedures of the criminal process that it cannot be allowed under any circumstances'.[232]

However, in this particular case, Justice Barak approved the privilege because he decided that the evidence was not essential for the defence.[233]

The precise meaning of the 'essentiality requirement' was discussed in several other cases.[234] However, the general rule was reaffirmed again in *Mazrib* case. Justice Dorner, for the majority, states that 'The court must direct a disclosure of evidence that is essential for the defence even if the harm to the public interest or to the state security is severe'.[235] Justice Cheshin, the dissenting judge, also agrees that 'the rule, therefore, that if the investigation material – that its disclosure might harm an important public matter and thus a privilege warrant was issued for it – is essential for the defence of the accused, the privilege must be removed'.[236]

C. The Relevance of the Israeli Experience to the UK

Two important points can be learnt from the Israeli experience: the lack of exclusion rule for intercept evidence and the emphasis on the fact that the state always has a choice to keep the information concealed by withdrawing from the indictment.

---

[231] Ibid 738-739.

[232] Ibid.

[233] 'It is found that the disclosure of the material is not essential for the defence, because it does not contain anything substantial that can help the defence in its argument regarding the admissibility of the confessions, and in contrast, the harm to the state security from the disclosure of the means of proof is substantial and evident.', ibid 743-744.

[234] See 64/87 *Va'anunu v The State of Israel* (BS); 1924/93 *Greenberg v The State of Israel* (BSP).

[235] 889/96 *Mazrib v The State of Israel* (CA) 443-444.

[236] Ibid 466-467.

i. Lack of Exclusion Rule for Intercept Evidence

The Israeli experience serves as yet another example to a jurisdiction in which intercept evidence is allowed. Such evidence was recognised as admissible for almost 30 years. Moreover, the Wiretapping Act 1978 was not a change from a previous exclusionary attitude toward this evidence, but rather an explicit recognition of its admissibility.

State security considerations in general, and the secrecy of the working methods in which intercept evidence is obtained in particular, are very dominant considerations in the Israel. Yet, unlike the UK, evidence that was legally-obtained using these methods is not automatically excluded. Thus, even though Israel faces more frequent terrorist attacks than the UK, a strict exclusion rule for intercept evidence was not deemed necessary.

ii. The Option to Withdraw from the Indictment

Maybe the more interesting insight that the Israeli experience has to offer is the emphasis on the choice that the state has in case the privilege is refused. In *Livny*, Barak mentions that even if the court decides to refuse the state's request for a privilege, the prosecution always has the choice to avoid the disclosure of the information by withdrawing from case and cancelling the indictment:

> Once the court decided that the evidence should be disclosed, the prosecution faces the dilemma whether to continue the criminal process or to cancel it. If the prosecution continues, it will have to disclose the evidence. If the prosecution thinks that the disclosure will harm the security state, it will have to bring about the stopping of the criminal process and sometimes even to the acquittal of the accused. [237]

In the later case *Mazrib*[238], both the Justice Dorner for the majority and the dissenting judge Justice Cheshin repeated this recognition that the state always has the choice to avoid disclosure by withdrawing from the indictment. Justice Dorner states that 'when the prosecution thinks that the public or security matter is more important than convicting the accused, the trial will be stopped or the accused will be acquitted'.[239]

Justice Cheshin goes even further:

> For all of these, we shall remember and not forget: a warrant to disclose the evidence does not mean enforcing the state to reveal and abandon its secrets to the entire world. A disclosure warrant only means that the state has to do 'self-examination': if it wants – it will disclose the evidence, if it does not want – it will not disclose the evidence. If the state chooses the first alternative – the disclosure alternative – we will know that according to the opinion of the state itself it is more preferable to convict the accused in the charges even in the price of the disclosure of the evidence. And if the state chooses the other alternative – the non-disclosure alternative – we will know that this 'important public interest' for which the state asked the privilege, reflects a novel interest; so novel

[237] *Livny* (n 2300) 736-737.

[238] *Mazrib* (n 235).

[239] Ibid 443-444.

> that is it worthy, in the state's opinion, that the accused will be acquitted and that secret information will not be revealed to everybody's eyes.[240]

This emphasis on the choice that the state has provides, in my view, an interesting insight. Instead of understanding the choice to be between exclusion and admission of intercept evidence, maybe the actual choice is between (1) a strict rule that always prevents the state to prosecute based on this evidence, and (2) a more flexible regime that allows the state to decide on a case-by-case basis whether the harm to the state security from disclosing this evidence is so significant that it would be better to avoid pressing the charges against the persons involved.

[240] Ibid 463-464.

THE OXFORD PRO BONO PUBLICO TEAM

The legal research on this project was conducted by a group of postgraduate law students, supervised by Professor Denis Galligan, under the auspices of the Oxford Pro Bono Publico programme. The students are: Lydia-Maria Bolani, Alex Chung, Ernesto J Feliz, Veronika Fikfak, Natacha Heffinck, Amit Pundik. For additional information please contact OPBP at opbp@law.ox.ac.uk.