a JUSTICE report

INTERCEPT EVIDENCE
Lifting the ban

Advancing access to justice, human rights and the rule of law

Intercept evidence: Lifting the Ban

a JUSTICE report

October 2006

For further information contact

Eric Metcalfe, Director of Human Rights Policy

email: emetcalfe@justice.org.uk direct line: 020 7762 6415

JUSTICE, 59 Carter Lane, London EC4V 5AQ tel: 020 7329 5100

fax: 020 7329 5055 email: admin@justice.org.uk website: www.justice.org.uk

Contents

Executive summary

- The UK is the only country in the common law world that prohibits completely the use of intercepted communications as evidence in criminal proceedings.

- Since 9/11, the lack of admissible evidence in terrorism cases has been cited by the government as justification for such exceptional measures as indefinite detention without trial and, more recently, the use of control orders involving the use of special advocates and secret evidence.

- This report looks in detail at the UK's ban on intercept evidence, and examines the arguments for and against allowing its use. The report also looks at the use of intercept material in 7 other common law countries with adversarial criminal procedures similar to the UK: Australia, Canada, Hong Kong, Ireland, New Zealand, South Africa and the United States.

- We conclude that the current ban is archaic, unnecessary and counter-productive. Outside the UK, intercept evidence has been used to convict Al-Qaeda cells in the United States following 9/11, the Five Godfathers of New York Crime, and war criminals before the International Tribunal on the Former Yugoslavia. Due to various loopholes in the current ban, intercept evidence is sometimes used successfully even in the UK. For example, recordings and transcripts of intercepted telephone conversations were used to help convict Ian Huntley of the Soham murders in 2003.

- The experience of other common law countries shows that the fears of the intelligence services that intercept evidence would lead to their interception capabilities being compromised are unfounded. Established common law principles of public interest immunity ('PII') work well in other countries to prevent the unnecessary disclosure of sensitive intelligence material, such as methods of interception and the identity of informants.

- We recommend that the ban on intercept evidence be lifted, and that the government overhaul the existing legal framework so that interception warrants are granted by judges rather than by the Home Secretary. Although we avoid making specific recommendations on this point, we also favour the establishment of a single interception warrant for both intelligence and law enforcement purposes whose product is admissible in criminal proceedings, rather than have separate intelligence warrants under which interceptions would continue to be inadmissible.

Acknowledgements

Founded in 1957, JUSTICE is a UK-based human rights and law reform organisation. Its mission is to advance justice, human rights and the rule of law. It is also the British section of the International Commission of Jurists.

JUSTICE wishes to thank Freshfields Bruckhaus Deringer for their help with researching Australian and Hong Kong law and for supporting the publication costs of this report. This project would not have been possible without their assistance and support. We are also very grateful to Bell Gully for their research on New Zealand law and to Oxford Pro Bono Publico for their research on intercept evidence in Canada, South Africa and the United States.

JUSTICE greatly appreciates the contribution made by those who presented papers on the use of intercept evidence at the JUSTICE/Sweet & Maxwell Conference on Counter-Terrorism and Human Rights on 28 June 2005: Anthony Arlidge QC of 18 Red Lion Court and Kingsley Hyland of the Crown Prosecution Service. We would also like to thank Professor Ivana Bacik of Trinity College Dublin for her assistance with the Irish law on the use of intercept evidence.

Please note that the views expressed in this report, and in particular the analysis and conclusions drawn, are those of JUSTICE.

This report was written by Dr Eric Metcalfe, Director of Human Rights Policy, JUSTICE, and researched by Gabrielle Guillemin, JUSTICE policy intern, and Emma Douglas, JUSTICE legal officer.

Introduction

1. In October 1586, Mary, Queen of Scots was convicted of treason for plotting to kill Elizabeth I. Among the evidence at her trial were enciphered letters, detailing her knowledge of Babington's plot, which had been intercepted by Walsingham, Elizabeth's Secretary of State and chief spy master.

2. It is one of the earliest – and most notorious – examples of intercept evidence being successfully used in English courts.

3. In October 2006, communications technology has advanced – and continues to advance – considerably beyond the sending of coded, hand-delivered letters. There are now, for instance, over 33 million landlines and over 65 million active mobile phone subscriptions in the UK.[1] As the technology has developed, so too has the interception capability of law enforcement and intelligence services. As is the case in many other countries, UK law currently permits police and other government agencies covertly to intercept telephone calls and other kinds of communication - including emails, faxes, text messages, VoIP[2] and ordinary post – in order to detect and prevent serious crime and acts of terrorism. In 2004, the Home Secretary issued 1849 warrants authorising the interception of communications, and a further 674 warrants continued in force from previous years.[3] (By way of comparison, the total number of federal and state wiretap authorisations in the entire United States in 2005 was 1773).[4]

4. However, although both communications technology and interception capability may have advanced far beyond that of Walsingham's day, the rules governing the admissibility of intercept material in UK courts are more conservative than they were in the 16th century. Although the UK – like nearly every other country in the world – allows the use of intercepted

---

[1] *The Communications Market* (Ofcom, August 2006), para 3.3.6 and fig 3.19

[2] Voice over Internet Protocol: the routing of telephone conversations (including videophone) over the internet or any IP network.

[3] Annex, *Report of the Interception of Communications Commissioner for 2004* (HC 549; SE/2005/203). A further 124 warrants were issued by the Scottish Executive in the same period. Note that the number of warrants may not itself disclose the true extent of interceptions: the 2004 report notes that 3101 modifications to warrants were made in the same period.

[4] *2005 Wiretap Report* (Administrative Office of the United States Courts, April 2006), p5. Note that the total UK figure for 2004 includes both telecommunications and postal intercepts (no further breakdown is publicly available), whereas the US figures only cover telecommunications intercepts.

communications for law enforcement purposes, it is virtually the only country to prohibit the use of intercepted material as evidence to help convict criminals and terrorists.[5]

5. By contrast, intercept evidence has been used in other countries to help convict many of those involved in serious organised crime and terrorism, including Al Qaeda cells operating in the United States following 9/11,[6] the Five Godfathers of the New York Mafia,[7] and war criminals in the Hague.[8] Indeed, despite the current UK ban, various loopholes allow the successful use of intercept evidence in UK courts in a limited number of cases. For instance, Ian Huntley was convicted of the Soham murders in December 2003 partly on the basis of intercepted telephone calls made between Huntley, his girlfriend Maxine Carr, and Huntley's mother.[9] Yet even the evidence of intercepted letters that convicted Mary Queen of Scots in 1586 would not now be admissible under the current law.[10]

6. The wisdom of barring potentially probative evidence of guilt from criminal proceedings would seem debatable enough, save that – since the 9/11 attacks – evidential difficulties in terrorism cases have been used by the government to justify various exceptional counter-terrorism measures, including the indefinite detention of foreign nationals without trial,[11] the use of control orders to impose 18 hour curfews on suspects without a criminal charge,[12] and extending the maximum period of pre-charge detention in terrorism cases to 28 days.[13]

---

[5] As shown in Part 3, the only common law jurisdiction with a comparable prohibition is Hong Kong. However, even Hong Kong allows the use of postal intercepts as evidence. Intercept evidence is technically admissible in the Republic of Ireland. However, as a matter of practice, it is not used by prosecutors in criminal proceedings.

[6] See para 93 below.

[7] See e.g. Jacobs and Gouldin, 'Cosa Nostra: The Final Chapter?'*Crime and Justice*, Vol. 25, 1999 (1999), pp. 129-189; 'Networks and Counter-Networks: The Criminal Prosecutions of the Sicilian and Neapolitan Mafia in the United States', *Mentis Vita* (2005).

[8] See judgment of the International Criminal Tribunal for the Former Yugoslavia in *Prosecutor v Radoslav Brdjanin*, 1 September 2004, Case No. IT-99-36-T. Brdjanin, a former Bosnian Serb political leader, was sentenced to 32 years imprisonment for torture, wilful killing and other crimes. In his trial, an objection was raised to the introduction of evidence obtained from intercepted communications on the basis that the interceptions had not been made lawfully. The trial chamber concluded that the intercept evidence was nonetheless admissible: see Decision on the Defence 'Objection to Intercept Evidence', 3 October 2003.

[9] See para 103 below.

[10] Intercepted communications under Part I of RIPA includes interceptions of communications sent via the postal network.

[11] Part 4 of the Anti-Terrorism Crime and Security Act 2001, now repealed by section 16 of the Prevention of Terrorism Act 2005. See below paras 28-30.

[12] See e.g. *JJ and others v Secretary of State for the Home Department* [2006] EWCA Civ 1141, in which the Court of Appeal ruled that the Secretary of State had no power to make orders against 6 individuals imposing 18 hour curfews under the Prevention of Terrorism Act 2006. See below paras 31-33.

[13] Section 23 of the Terrorism Act 2006. See below paras 34-36.

7. In light of these measures and the evidential difficulties in terrorism cases that have been used to justify them, the issue of intercept evidence has become the subject of keen public debate. A significant number of senior police officers, prosecutors, judges and politicians have now called for intercept evidence to be used in criminal trials.[14] Indeed, the Home Affairs Committee noted in July 2006 that 'outside the Government there is universal support for the use of intercept evidence in the courts'.[15] Despite a succession of reviews, however, the government has yet to announce a shift in its position.

8. The use of intercept evidence raises a number of human rights issues, chiefly the right to a fair trial and the right to privacy, protected under the Human Rights Act 1998 by Articles 6 and 8 of the European Convention on Human Rights respectively. The way in which interceptions are regulated, and the extent to which any unused intercept material is disclosable to defendants, both impact on fundamental rights. But the failure to allow intercept evidence also raises human rights issues, especially when exceptional counter-terrorism measures are being justified by reference to the difficulty of obtaining sufficient admissible evidence to prosecute terrorist offences in the criminal courts.

9. The debate over intercept evidence engages other interests as well. There is the public interest in ensuring that interception capabilities are not compromised, so that intercepted communications continue to be of value in detecting and preventing serious crime and acts of terrorism. Most of all, there is the public interest in the fair administration of justice: ensuring that the adversarial criminal process works effectively to protect fundamental rights, convict the guilty and acquit the innocent.[16]

10. JUSTICE has long been concerned with these issues. In 1998, as part of a broader study on the human rights aspects of covert surveillance by police,[17] we observed that there was a 'growing consensus' that the ban on intercept evidence was 'now unsatisfactory'[18] and recommended the ban should be lifted in order to bring UK law into line with the position in a

---

[14] See Appendix.

[15] House of Commons Home Affairs Committee, *Terrorism Detention Powers* (HC 910, 3 July 2006), para 116.

[16] See e.g. Lord Hobhouse of Woodborough, *Arthur J.S Hall and Co. v. Simons* (2000) 3 All ER 673: 'Even though the criminal process is formally adversarial, it is of a fundamentally different character to the civil process. Its purpose and function are different. It is to enforce the criminal law. The criminal law and the criminal justice system exists in the interests of society as a whole. It has a directly social function. It is concerned to see that the guilty are convicted and punished and those not proved to be guilty are acquitted. Anyone not proved to be guilty is to be presumed to be not guilty. It is of fundamental importance that the process by which the defendant is proved guilty shall have been fair and it is the public duty of all those concerned in the criminal justice system to see that this is the case. This is the public interest in the system'.

[17] *Under Surveillance: Covert policing and human rights standards* (JUSTICE, 1998)

[18] Ibid, p 76.

number of other countries including the United States, Canada and Australia.[19] Whereas our 1998 report made this recommendation as one of a range of issues, however, this report focuses exclusively on the question of intercept evidence: analysing the arguments for and against the current ban and setting out the comparative law under which intercept evidence is used in other common law countries:

- ***Part 1*** of this report provides an overview of the intercept evidence debate, including the definition of intercepted communications and the legal framework provided by the Regulation of Investigatory Powers Act 2000.

- ***Part 2*** examines the various arguments put forward by the government justifying the ban, and presents arguments in favour of its use.

- ***Part 3*** looks at the use of intercept evidence under the European Convention on Human Rights and in the other common law jurisdictions that use the same adversarial system of criminal proceedings as the UK: Australia, Canada, Hong Kong, Ireland, South Africa and the United States.

- The ***Appendix*** sets out statements of support for the use of intercept evidence made by senior police, prosecutors, lawyers and politicians. It also contains a table setting out the comparative use of intercept evidence in common law jurisdictions.

[19] Ibid, recommendation 15.

PART I

What is intercept evidence?

11. An ***'intercept'*** is the term used to describe the covert interception of a private communication by intelligence services or law enforcement agencies. The interception of telephone calls – e.g. by use of wiretaps, etc – is perhaps the best-known example. However, under the Regulation of Investigatory Powers Act 2000 ('RIPA'), ***'intercepted communications'*** also covers other kinds of communications, including mobile phones, email, fax and ordinary post.[20]

12. ***'Intercept evidence'*** refers to the use of information gained from intercepted communications as evidence in civil or criminal proceedings. However, UK law currently prohibits the use of any evidence in legal proceedings in the UK which discloses or tends to disclose either the fact that a given communication has been intercepted (e.g. the fact that the police had been listening in on a particular person's phone calls) or the contents of that call (i.e. what was actually said in the phone calls).[21]

13. The use of intercepted communications as evidence is typically distinguished from the use of intercepts purely for ***intelligence*** purposes – e.g. to enable law enforcement and intelligence bodies to gain information on the activities of those suspected of involvement in serious crime and threats to national security. As we will see below, however, this is not such a hard and fast distinction: information gathered for one purpose may be equally useful for another.

14. Intercept evidence is sometimes confused with information gained from other kinds of ***covert surveillance*** by law enforcement or intelligence services, e.g. eavesdropping on suspected terrorists using bugging devices, via a concealed microphone worn by an informant or undercover officer, or monitoring suspects' activities using a hidden camera.[22] As a result, it is often wrongly assumed that *any* kind of surveillance is inadmissible in UK courts because of the ban on intercept evidence.[23]

15. In fact, the interception of communications is simply *one* type of covert surveillance among the many used by law enforcement agencies and intelligence services in order to prevent and

---

[20] See section 2 of the Regulation of Investigatory Powers Act 2000.

[21] See paras 37-42 below.

[22] RIPA distinguishes between directed and intrusive surveillance: see section 26 and Part II of RIPA generally. See also Hong Kong Law Reform Commission, *Privacy: the Regulation of Covert Surveillance* (March 2006), p 65 setting out the distinction between intercept and covert surveillance in general.

[23] For further details of the exceptions to the ban on intercept evidence, see paras 37-42 and 102 below.

detect serious crime (including terrorist activity). However, for reasons that are examined in detail below, UK law has long treated the use of information gained from intercepted communications differently from other forms of surveillance.

Why is intercept evidence controversial?

16. The covert interception of private communications by government has long been controversial. Indeed, the use of such interceptions and the controversy surrounding them are probably as old as the means of communication themselves. According to the 1953 Privy Council report on intercepted communications in the UK, 'the first public reference of the Secretary of State authorising the opening of letters is the Proclamation of May 25th, 1663'.[24] President Lincoln authorised the tapping of telegraphs during the American Civil War.[25] And, as the European Court of Human Rights noted in 1984, 'the power to intercept telephone messages has been exercised in England and Wales from time to time since the introduction of the telephone'.[26] As early as 1844, a committee of the House of Commons noted:[27]

> the strong moral feeling which exists against the practice of opening Letters, with its accompaniments of mystery and concealment

17. However, the mere fact of governmental intrusion into personal privacy is not enough to explain the controversy over intercept evidence. As noted above, evidence drawn from other kinds of covert surveillance by law enforcement, such as bugging or video surveillance, is readily admissible in English courts with no obvious opposition from the security services and no apparent outcry from the public. In any event, any interference with privacy that flowed from using intercept material as evidence must be seen as secondary to the core interference with private communications, which is the fact of interception itself.

18. Rather than privacy being the only source of concern, the controversy over the ban on intercept evidence in the UK arises for at least five reasons:

    (a) The covert interception of telephone calls, letters and email by government involves a significant intrusion into personal privacy;

---

[24] *Report of the Privy Councillors appointed to inquire into the interception of communications* (Cmnd 283, October 1957), para 9. See also paras 51 ('the power to intercept letters has been exercised since the earliest times') and 147 ('the power to open letters has been exercised in this country for many hundreds of years').

[25] See David Homer Bates, *Lincoln in the Telegraph Office: Recollections of the United States Military Telegraph Corps During the Civil War* (London: University of Nebraska Press, 1995).

[26] *Malone v United Kingdom* (1984) 7 EHRR 14 at para 28.

[27] Report of the Secret Committee of the House of Commons, cited in the Birkett report, n24 above, para 133.

(b) Intercepted communications are nonetheless a valuable source of information for law enforcement agencies and intelligence services in the fight against terrorism and serious organised crime, and therefore the interference with individual privacy may be justified so long as the interceptions are lawful and proportionate;

(c) Those engaged in the business of lawfully intercepting communications are extremely keen to prevent information concerning their methods and interception capabilities becoming publicly known – in particular, to those who may be the subjects of interception;

(d) The UK is the only common law jurisdiction to prohibit completely[28] the use of intercepted communications in criminal proceedings; and

(e) Since 9/11, the government has justified a succession of highly exceptional counter-terrorism measures (including control orders and indefinite detention without trial) by reference to the evidential difficulties in bringing criminal prosecutions for terrorism offences.

19. In particular, the government is refusing to admit intercepts as evidence in terrorism cases while continuing to cite the lack of admissible evidence as justification for introducing exceptional counter-terrorism measures.

20. The precise nature of the statutory ban on intercept evidence is set out in the following section. The arguments for and against lifting the ban (including those made from privacy concerns) are considered in Part 2. The comparative use of intercept evidence in other common law jurisdictions is set out in Part 3. The remainder of this section looks briefly at:

    (i) the value of intercepted communications for law enforcement;
    (ii) evidential difficulties in terrorism cases; and
    (iii) exceptional measures justified by lack of admissible evidence.

The value of intercepted communications for law enforcement

21. There is abundant evidence that the use of intercepted communications is considered a valuable tool in the detection and prevention of crime – including acts of terrorism – by law enforcement agencies in the UK and elsewhere.

22. As early as 1953, a committee of Privy Councillors appointed to review the law relating to intercepted communications found that interception 'has proved very effective in the detection of major crimes, customs frauds on a large scale and serious dangers to the security of the State'.[29] The government's 1980 White Paper on the same issue stated:[30]

> the increase of crime, and particularly the growth of organised crime, the increasing sophistication of criminals and the ease and speed with which they can move about have made telephone interception *an indispensable tool* in the investigation and prevention of serious crime.

23. The following year, Lord Diplock, who had been appointed by the government to monitor the arrangements for interception (a role that subsequently became the Interception of Communications Commissioner), reported:[31]

> The interception of communications, particularly telephone conversations, remains *an effective, indeed an essential, weapon* in the armoury of those authorities responsible for the maintenance of law and order and the safety of the realm. Major crime has become more highly organised, international trafficking in drugs brings enormous profits, and terrorism has become a world wide problem; and all of this has made it more necessary for the members of criminal gangs in each of these categories to communicate with one another by telephone about their activities and plans.

24. In a similar vein, the government's 1999 consultation paper on intercepted communications stated:[32]

> In most developed countries, interception of communications is used by the law enforcement, security and intelligence agencies in their work against serious crime and threats to national security, including terrorism. The UK is no exception. *Interception represents an indispensable means of gathering intelligence against the most sophisticated and ruthless criminals.*

---

[28] See Part 3: Hong Kong prohibits evidence of telecommunication intercepts but not postal intercepts. The Republic of Ireland does not formally prohibit the use of intercept evidence, but neither do prosecutors seek to rely on such material as evidence in criminal proceedings.

[29] Birkett report, n24 above, para 123.

[30] Home Office, *The Interception of Communications in Great Britain* (Cmnd 7873, April 1980), para 21. Emphasis added.

[31] Lord Diplock, quoted in *Interception of Communications in the United Kingdom: a Consultation Paper* (Home Office:June 1999, Cmnd 4368), para 1.3. Emphasis added.

[32] 1999 Consultation paper, ibid, p 1. Emphasis added.

Evidential difficulties in terrorism cases

25. In 1996, the independent reviewer of terrorism legislation, Lord Lloyd of Berwick, noted that:[33]

> One of the themes which has persisted throughout [this] Inquiry is *the difficulty of obtaining evidence on which to charge and convict terrorists*, particularly those who plan and direct terrorist activities without taking part in their actual execution. This has proved to be a serious weakness in the anti-terrorist effort, especially in Northern Ireland. In many cases the leaders of the paramilitary organisations may be well known enough to the police, but there is insufficient evidence to convict them.

26. Following the introduction of the Anti-Terrorism Crime and Security Act 2001, a committee of Privy Councillors headed by Lord Newton was appointed to review the Act and its operation. They reported their findings in December 2003, and explained the failure to prosecute those subject to indefinite detention under Part 4 of the Act in the following terms:[34]

> It has not been represented to us that it has been impossible to prosecute a terrorist suspect because of a lack of available offences. The inhibiting factor … seems to be that *intelligence on which suspicion of involvement in international terrorism is based*
>
> a. *would be inadmissible in co*urt; or
>
> b. *the authorities would not be prepared to be prepared to make it available in open court, for fear of compromising their sources or methods*.

Exceptional measures justified by lack of admissible evidence

27. Since the 9/11 attacks, at least three significant exceptions to established due process and fair trial rights have been introduced and justified by the government by reference to evidential difficulties in terrorism cases:

---

[33] Lord Lloyd of Berwick, *Inquiry into Legislation Against Terrorism, Vol 1*(October 1996: Cm 3420), para 7.1. Emphasis added.

[34] *Report of the Privy Counsellors Review of the Anti-Terrorism Crime and Security Act 2001* (HC 100: 18 December 2003), para 207, emphasis added. This was endorsed by the Joint Committee on Human Rights (JCHR), in its July 2004 report (*Review of Counter-Terrorism* Powers (HL 158/HC 713)) criticising the proposed creation of further terrorist offences noting that it was 'difficult to see how the existence of such an offence would overcome the obstacles to prosecution identified by the Newton Report, in particular the problem that the evidence relied on in relation to a suspected international terrorist is usually intelligence material which is either inadmissible as evidence in a criminal court, or material which the authorities do not wish to disclose for fear of compromising sources or methods' (para 67).

(i) indefinite detention of foreign terrorist suspects;
(ii) the use of control orders against persons suspected of involvement in terrorism; and
(iii) the extension of the maximum period of pre-charge detention in terrorism cases from 14 days to 28 days.

Indefinite detention of foreign terrorist suspects

28. Passed three months after 9/11, the Anti-Terrorism Crime and Security Act 2001 ('ATCSA') represented the government's legislative response to those attacks. In particular, Part 4 of the Act allowed the Home Secretary to detain indefinitely without trial those foreign nationals whom he had certified as suspected international terrorists. In order to enact Part 4, the government derogated from the right to liberty under Article 5(1) of the European Convention on Human Rights ('ECHR') on the basis that the threat of terrorism from Al Qaeda represented 'a public emergency threatening the life of the nation' (adopting the language of Article 15 of the Convention).[35] Then-Home Secretary David Blunkett MP was challenged during parliamentary debate to explain why those suspected of terrorism were not simply charged with terrorist offences:[36]

> Does the Home Secretary accept that there is a sea of difference between SIAC being used to deal with issues of deportation—with all the problems that SIAC has as a review body—and its being used to review decisions to incarcerate and imprison, indefinitely, without trial and, indeed, without charge? If evidence exists against the people about whom we have heard, why are they not being charged and tried in this country?

Blunkett explained:[37]

> If the evidence that would be adduced and presented in a normal court were available, of course we would use it, as we have done in the past …. [However] *in some cases the nature of the evidence from the security and intelligence services will be such that it would put at risk the operation of those services and the lives of those who act clandestinely to help them if that evidence were presented in normal open court.*

29. Lord Rooker, a Home Office Minister, justified the measures to the House of Lords in far blunter terms:[38]

---

[35] See Human Rights Act 1998 (Designated Derogation) Order 2001 (SI 3644).

[36] Robert Marshall-Andrews MP: Hansard, HC Debates, 19 November 2001, Cols 28-29.

[37] Hansard, HC Debates, 19 November 2001, Cols 28-29. Emphasis added.

> If we could prosecute on the basis of the available evidence in open court, we would do so. *There are circumstances in which we simply cannot do that because we do not use intercept evidence in our courts.*

30. In December 2004, the Judicial Committee of the House of Lords held by an 8-1 majority that the provisions of Part 4 allowing indefinite detention of foreign suspected terrorists without trial were incompatible with the right to liberty under Article 5 ECHR and the right to non-discrimination under Article 14.[39]

Control orders

31. Following the December 2004 judgment of the House of Lords in the Belmarsh case,[40] the government agreed to bring forward fresh legislation to replace indefinite detention under Part 4 of ATCSA. The Prevention of Terrorism Act 2005, passed the following March, introduced the system of control orders which remains in force today – enabling the Home Secretary to impose restrictions on those individuals he suspects of involvement in 'terrorist-related activity'. Under the Act, conditions imposed by way of a non-derogating order may include restrictions on a suspect's place of residence, movement, employment, personal property, association and communication with others.[41] In the case of derogating orders, the Home Secretary can apply to the court for an order imposing conditions tantamount to house arrest.[42]

32. As his predecessor had done in parliamentary debates over indefinite detention, the then-Home Secretary Charles Clarke MP referred to the evidential difficulties associated with terrorism cases as justification for the introduction of control orders:[43]

> I want to make it clear that prosecution is, and will remain, our preferred way forward when dealing with all terrorists. All agencies operate on that basis, and will continue to

---

[38] Hansard, HL Debates, 27 November 2001: Column 146. Emphasis added.

[39] *A and others v Secretary of State for the Home Department* [2004] UKHL 56, known as 'the Belmarsh case'.

[40] Ibid.

[41] Section 2 of the 2005 Act governs the making of non-derogating orders. The restrictions which may be imposed are set out under section 1(4).

[42] See section 4.

[43] Hansard, HC Debates, 26 Jan 2005: Col 305. Emphasis added. The Lord Chancellor Lord Falconer similarly cited 'the evidential problems in proving the link between the individual, his activity and terrorism' in the Lords debates on the Prevention of Terrorism Bill (Hansard, HL Debates, 1 March 2005 : Column 119).

do so, but all of us need to recognise *that it is not always possible to bring charges, given the need to protect highly sensitive sources and techniques.*

33. As recently as September 2006, the government reiterated its justification:[44]

> Control orders are used in cases where there is no evidence available that could realistically be used for the prosecution of an individual for an offence relating to terrorism.

Extension of pre-charge detention to 28 days

34. Most recently, the evidential difficulties in terrorism cases were cited as justification for extending pre-charge detention in such cases from 14 days to 28 days under section 23 of the Terrorism Act 2006. Specifically, police and government cited the difficulty in gathering sufficient admissible evidence within the existing 14 day time limit:[45]

> Public safety demands earlier intervention, and so the period of evidence gathering that used to take place pre-arrest is often now denied to the investigators. This means that in some extremely complex cases, evidence gathering effectively begins post-arrest, giving rise to the requirement for a longer period of pre-charge detention to enable that evidence gathering to take place, and for high quality charging decisions to be made.

35. As was noted in parliamentary debates on the 2006 Act,[46] intercept material is often used by police as grounds for reasonable suspicion that an individual is a terrorist, justifying that person's arrest under the Terrorism Act 2000.[47] As the Chief Constable of Greater Manchester Police told the Home Affairs Committee in 2004:[48]

> If you have information from an informer, if you have technical surveillance evidence, if you have intercept evidence, there is a whole series of things which actually says,

---

[44] The Government Reply to the Fourth Report from the Home Affairs Committee Session 2005-2006, HC910 on Terrorism Detention Powers (Cm 6906, September 2006), para 29).

[45] Letter from Anti-Terrorist Branch of the Metropolitan Police, 5 October 2005, printed as an appendix to the Home Affairs Committee, *Terrorism Detention Powers* (HC 910: June 2006).

[46] See e.g. Hansard, HC Debates, 26 October 2005 : Column 362, Mark Oaten MP: 'If the police had arrested someone but could not employ the evidence that they had used for arrest to charge them with an offence, a change in the Government's policy on intercept communication would be key'.

[47] Section 41(1) Terrorism Act 2000. See also section 24 of the Police and Criminal Evidence Act 1984, as amended by the Serious Organised Crime and Police Act 2005.

[48] Evidence to the Home Affairs Committee, 8 July 2004, Q59.

> 'This group of people or this individual are involved in the preparation for some form of act of terrorism', then we will arrest.

36. However, because intercepts are inadmissible as evidence, they cannot be used as the basis for preferring criminal charges for terrorist offences. Using the hypothetical example of a suspected terrorist who is arrested immediately prior to carrying out an attack, where the sole basis for suspicion of terrorist activity is intercept evidence, the Chief Constable explained:[49]

> We have got it on intelligence; we have got it on the telephone intercept. We would have enough intelligence and information to justify that person's arrest. Could we convict that person without an admission? Not a hope in hell because they have not actually done anything wrong.

The existing legal framework

37. The statutory prohibition on intercept evidence is contained in Part 1 of the Regulation of Investigatory Powers Act 2000 ('RIPA'), which regulates interceptions of any communication made via:[50]

    (a) a public postal service (e.g. Royal Mail)

    (b) a public telecommunication system (e.g. phone and internet); or

    (c) a private telecommunication system (e.g. an internal phone system or computer network)

38. Section 5 of RIPA allows the Home Secretary to issue warrants authorising the interception of communications where various conditions are met, including where he is satisfied that the warrant is necessary in the interests of national security or the purposes of detecting or preventing serious crime.[51] However, lawful interception of communications without a warrant is also possible in certain circumstances, including:

    (a) where both parties consent to the interception (e.g. notification that calls made to a call-centre are likely to be recorded);[52]

---

[49] Evidence to the Home Affairs Committee, 8 July 2004, Q49.

[50] See e.g. ss1(1) and (2) of RIPA.

[51] Sections 5(3)(a) and (b).

[52] Section 3(1) RIPA.

(b) where one party consents to the interception (e.g. one party is recording the conversation without the other's knowledge) and the interception has been authorised as *directed surveillance* rather than an interception;[53]

(c) where the interception takes place on a private telecommunications network with the consent of the controller of the system;[54]

(d) where the communications are made to or from a prison or psychiatric hospital.[55]

39. Section 17 of RIPA sets out the statutory bar on using intercept material in court. Section 17(1)(a) provides that:

> no evidence shall be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings which (in any manner) …. discloses, in circumstances from which its origin [from an interception warrant or an unlawful interception] may be inferred, any of the contents of an intercepted communication or any related communications data;

40. Section 17(1)(b) similarly prohibits any evidence that would even 'tend to suggest' that an interception warrant has been applied for, or issued, or is about to be issued, etc.

41. However, the prohibition under section 17 does *not* extend to interceptions made *outside* the UK. Therefore, there is no bar to admitting intercept evidence lawfully obtained in foreign jurisdictions. As Lord Mustill noted in the case of *R v P* concerning the predecessor to RIPA, the Interception of Communications Act 1985:[56]

> The law of country 'A' under which these intercepts were made does not treat secrecy as paramount; it permits, subject to judicial supervision, the use of intercepts in evidence. There is no basis for the argument that there is a rule of English public policy which makes this evidence, which is admissible in country 'A', inadmissible in England.

---

[53] See sections 3(2) and 48(4).

[54] Sections 1(6) and 3(3).

[55] See subsections 4(4)-4(6).

[56] (2001) 2 All ER 58. Although the prohibition on intercept evidence under RIPA is more comprehensive than that under the 1985 Act, for the purposes of the territorial extent the provisions are identical.

42. Equally, as the Newton Committee observed, section 17 does not prohibit communications intercepted in the UK being admitted into evidence in *foreign* courts, assuming that the intelligence and security services are prepared to provide them.[57]

[57] Newton Report, n34 above, para 210.

PART 2

Why is there a ban on intercept evidence? Government justifications for the ban

43. The policy of banning intercepted communications as evidence in criminal proceedings is a long-standing one. It has not, however, existed since time immemorial. As Lord Lloyd notes:[58]

> the 'privy letters' of Mary Queen of Scots to the French court were intercepted and deciphered by Walsingham, and used to great effect at her trial.

44. The 1953 Privy Council report on interceptions similarly listed several celebrated cases from the 18th century in which intercepted letters were used in evidence:[59]

> In the year 1758, Dr. Hensey, a physician, was tried on a charge of high treason, being accused of treasonable correspondence with the enemy. The principal evidence on which he was convicted was that of a letter carrier and a Post Office clerk, the latter of whom had opened Dr. Hensey's letters and delivered them to the Secretary of State.

45. By contrast, although it appears that 'the power to intercept telephone messages has been exercised in England and Wales from time to time since the introduction of the telephone',[60] there is no historical reference to telephone intercepts ever being put forward as evidence in criminal proceedings and by 1953 it had become 'the settled policy of the Home Office' that:[61]

> save in the most exceptional cases, information obtained by the interception of communications should be used only for the purposes of detection, and not as evidence in a Court or in any other Inquiry.

46. Despite this long-established practice against admitting intercept evidence, the current statutory ban dates only from 1985 when the Interception of Communications Act was passed following an adverse judgment by the European Court of Human Rights.[62] A consultation paper on intercepted communications was issued in 1999[63] following another adverse

---

[58] House of Lords Liaison Committee, 1st Report, HL Paper 29: 18 July 2005

[59] Birkett Report, n24 above, para 149.

[60] *Malone v United Kingdom* (1984) 7 EHRR 14 at para 28.

[61] Birkett report, n24 above, para 92.

[62] See *Malone,* n60 above and para 109 below. See also *Malone v Metropolitan Police Commissioner* [1979] 2 All ER 629 at 649 where Sir Robert Megarry VC observed that 'telephone tapping is a subject which cries out for legislation'.

[63] See 1999 Consultation paper, n30 above.

judgment from Strasbourg.[64] Nonetheless, the ban on intercept evidence was maintained in the Regulation of Investigatory Powers Act 2000.

47. Since the 9/11 attacks, the issue of intercept evidence has become increasingly prominent in parliamentary and public debate. Various amendments have been put forward to allow its use, including in debates during the passage of the Serious Organised Crime and Police Act 2005,[65] and the Terrorism Act 2006.[66] In addition, the Interception of Communications (Admissibility of Evidence) Bill was put forward by Lord Lloyd as a Private Members Bill in October 2005.[67] All have been unsuccessful.

48. Despite what has been described as 'universal support' for the use of intercept evidence,[68] the government has so far refused to lift the ban.[69] It has instead limited itself to a promise to keep the matter under review and an undertaking from the Home Secretary to:[70]

> find, if possible, a legal model that would provide the necessary safeguards to allow intercept material to be used as evidence.

In the absence of positive government proposals to allow its use, the government has continued to muster a wide range of arguments against lifting the ban on intercept evidence. The primary argument is that allowing such evidence would compromise interception capabilities. However, a variety of secondary arguments have also been put forward, including the claim that intercept evidence would be unlikely to show the guilt of suspects; that its use would harm the close relationship between the security and intelligence services and law enforcement bodies in the UK; that it would led to an intolerable burden being placed on courts and prosecutors; and so forth. This section critically examines the main arguments that have been deployed by the government and others against allowing the use of intercept evidence in court. The subsequent section will present positive arguments in favour of lifting the ban.

---

[64] *Halford v United Kingdom* (1997) 24 EHRR 523, para 51. See further para 112 below.

[65] See e.g. Hansard, Standing Committee D, 18 January 2005: Col 205.

[66] See Hansard, HL Debates, 13 December 2005 : Column 1217.

[67] Hansard, HL Debates, 10 October 2005 : Column 12.

[68] House of Commons Home Affairs Committee, *Terrorism Detention Powers* (HC 910, 3 July 2006), para 116.

[69] See e.g. written ministerial statement on intercept evidence, 26 Jan 2005, Col 18WS

[70] Rt Hon Charles Clarke MP, Hansard, HC Debates, 2 February 2006 : Column 479.

Intercept evidence would 'compromise methods of interception'

49. The primary argument advanced by opponents of intercept evidence is that disclosure of intercept material would reveal to suspected criminals and terrorists the *methods* by which their communications have been intercepted. Even if the methods themselves were not disclosed, it is argued, the use of intercept evidence would present an unacceptable risk that defendants might infer the methods used from the particular instances in which their communications were intercepted. The consequent harm would be a weakening of interception capabilities, as suspects develop new measures to avoid interception, and lessen the value of interceptions in general as a tool in the fight against serious crime and terrorism. The 1999 consultation paper on interceptions summarised the concern as follows:[71]

> exposure of interception capabilities will educate criminals and terrorists who will then use greater counter interception measures than they presently do. This would mean that any advantage gained by repeal would be short lived and would make interception operations more difficult in the longer term.

50. Concern over compromising interception capabilities was one of the main justifications advanced by government for retaining the ban on intercept evidence during debates on the Regulation of Investigatory Powers Bill in 2000. As one government whip argued:[72]

> [I]t is vital that the existing capability is protected. Exposure of interception capabilities would or might educate criminals and terrorists who might then use greater counter-interception measures than they presently do. We believe that it is vital that the existing capability is protected and that the exposure of interception capabilities, which would result, as night follows day, from a repeal of the prohibition, would educate criminals and terrorists. They would certainly use greater counter-interception measures than they presently do and the value of interception as an investigative tool — it is a valuable investigative tool, particularly against the most serious criminals and terrorists — would be seriously damaged. For those reasons, we are not convinced

---

[71] 1999 Consultation paper, n30 above, para 8.3

[72] Lord Bach, Hansard, HL Debates, 19 June 2000, col 111. See also e.g. Sir Stephen Lander, chair of the Serious Organised Crime Agency and former director of MI5: 'The risk … is that by opening [intercept material] up to due process and proper examination by the courts you will expose what we can do and what we cannot do'; quoted in 'Turn the tap on' by Clare Dyer, *The Guardian*, 22 February 2005; See also the former Secretary of State for Defence, Lord Robertson, in debates on the Terrorism Bill, Hansard, HL Debates, 13 December 2005 : Column 1219: 'The fact is that communications of all sorts are becoming ever more sophisticated, complex, concealed and surmountable. The criminal classes present a constant challenge in their efforts to stay ahead of those who stand for an ordered rather than a disordered society. If we were to expose the methods by which information is gathered, as inevitably we would have to do if the law was changed in the form being suggested, we would suffer more and be in much greater danger'.

that a change to an evidential regime would involve a rise in criminal convictions in any more than the short term. Criminals and terrorists would become 'wise' to it.

51. Indeed, it seems likely that the concern over revealing too much about the practice of interceptions is at the root of the long-standing policy against using intercepts as evidence. As Lord Mustill observed in 1994:[73]

> Those who perform the interceptions wish to minimise the dissemination of the fact that they have been performed, since it is believed that this would diminish the value of activities which are by their nature clandestine. *We need not consider to what extent this preoccupation with secrecy at all costs is soundly based for it has been treated as axiomatic for decades, if not longer.*

52. However, the argument that intercept evidence would reveal too much about interception capabilities seems to us profoundly misplaced for at least three reasons:

(i) suspected criminals and terrorists are already generally aware of interception capabilities;
(ii) interception capabilities can by protected by public interest immunity principles; and
(iii) there is no evidence that PII principles have failed to protect interception capabilities in other common law jurisdictions

[73] *R v Preston* (1994) AC 130 at p 163. Emphasis added.

General awareness of interception capabilities among suspected criminals and terrorists

53. First, it appears to assume, wrongly, that those involved in terrorism or serious crime are not already highly alert to the possibility that their phone calls and emails are vulnerable to interception. As Lord Lloyd noted in his 1996 report, 'sophisticated criminals are all well aware are that their telephones are, or may be, tapped'.[74] Nonetheless, there is no evidence that this general awareness of interception capabilities (if not their precise extent) has led criminals and terrorists to stop using telecommunications when carrying out their activities. As the government's own 1999 Consultation paper makes clear:[75]

> It is virtually impossible to organise a complex crime without communicating over public networks, and this is particularly true where there is an international dimension, *as is increasingly the case*.

54. The concern that intercept evidence would compromise methods of interception was similarly dismissed by the Head of Specialist Operations (including the Anti-Terrorist Branch) of the Metropolitan Police, Assistant Commissioner Andy Hayman, in evidence to the Home Affairs Committee in February 2006:[76]

> I originally started off by being fairly unsupportive of the notion of using [intercept] material, mainly on the basis that it was starting to disclose methodology to the other side. I think that is now well and truly worn-out because I think most people are aware of that. It does not stop them still talking but they are aware of the methodology so that is a lightweight argument.

55. For the reasons we outline below,[77] we think there is no likelihood that lifting the ban on intercept evidence will compromise methods of interception. Even so, the supposition that suspected criminals and terrorists might learn about methods of interception through disclosure in UK courts is wholly undermined when one considers the international nature of

---

[74] Lloyd report, n33 above, para 7.17

[75] 1999 Consultation paper, n30 above, para 1.3, emphasis added. See also Lloyd report, n33 above, para 7.17: 'If intercept evidence were to be used in court in one or two terrorist cases a year, I cannot believe that drug dealers would learn anything that they do not already know. As for the fear that criminals would cease to use the telephone altogether, I regard this as fanciful. Drug dealers planning an importation, or terrorists planning to plant a bomb, must communicate with each other and with those who are directing the operation by some means. It cannot be done by pigeon post'.

[76] Evidence to the Home Affairs Committee, Q224, 28 February 2006.

[77] See paras 56-62 below.

modern terrorism and serious organised crime[78] and the use of intercept evidence in other jurisdictions. Since intercepted communications are admissible as evidence in the overwhelming majority of countries throughout the world, and even foreign intercepts are admissible in the UK, it is almost certainly the case that those involved in international terrorism and serious organised crime in this country are already as well-versed in counter-interception methods as they are ever likely to be and that introduction of intercept evidence in the UK would make no difference to their methods of communication. As Andrew Mitchell MP noted in parliamentary debates on the Serious Organised Crime and Police Bill, the belief that intercept evidence would lead to an increase in counter-interception methods:[79]

> assumes that British serious criminals are a peculiarly insular lot whose information gathering does not penetrate far overseas.

Interception capabilities can by protected by public interest immunity principles

56. Secondly, opponents of intercept evidence appear either to dramatically understate or to ignore altogether the ability of existing safeguards to protect sensitive intelligence capabilities from being revealed in court proceedings. In cases involving serious organised crime, for instance, prosecutors regularly rely on established principles of public interest immunity ('PII') in order to prevent details of methods of covert surveillance, including the identity or even the existence of informants, from being disclosed to defendants. Yet, despite the regular use of surveillance evidence in such cases, we are not aware of any claim that existing PII rules have failed adequately to protect methods, sources or informants, or that or that covert surveillance techniques used by law enforcement and intelligence agencies in the UK have been compromised as a result.

57. Although the primary rule of disclosure in criminal proceedings is that the prosecution must disclose to the accused any material 'which might reasonably be considered capable of undermining the case for the prosecution against the accused or of assisting the case for the accused',[80] section 3(6) of the Criminal Procedure and Investigations Act 1996 prohibits the court from disclosing any material that it concludes is not in the public interest. Furthermore, the Code of Practice under Part 2 of the 1996 Act,[81] the Attorney General's guidelines on the disclosure of information in criminal proceedings, and the Joint Operational Instructions for the

---

[78] See e.g. Deputy Assistant Commissioner of the Metropolitan Police and National Coordinator of Terrorism Investigations Peter Clarke: 'Far from being domestic, [the current terrorist threat] is global in origin, global in ambition and global in reach', The Times, 'Special Branch absorbed into counter-terror unit', by Sean O'Neill 3 October 2006.

[79] Hansard, HC Debates, 7 Feb 2005, Col 1238.

[80] Section 3(1)(a) of the 1996 Act as amended by section 32 of the Criminal Justice Act 2003.

[81] See Criminal Procedure and Investigations Act 1996 (Code of Practice) Order 2005 (SI 2005/985).

Disclosure of Unused Material[82] all provide detailed guidance on the procedures whereby the prosecution may apply to the court to prevent the disclosure of sensitive material.[83] In addition, there is no obligation at all to disclose any sensitive material which is 'either neutral in its effect or which is adverse to the defendant, whether because it strengthens the prosecution or weakens the defence'.[84] As Lord Bingham noted in *R v H*, the most common justification for non-disclosure is the protection of covert surveillance techniques and capabilities:[85]

> The public interest most regularly engaged is that in the effective investigation and prosecution of serious crime, which may involve resort to informers and under-cover agents, or the use of scientific or operational techniques (such as surveillance) which cannot be disclosed without exposing individuals to the risk of personal injury or jeopardising the success of future operations.

58. The PII procedure in criminal cases is intended to strike a balance between the defendant's right to a fair trial (and the interests of justice in general), on the one hand, and the need to prevent the disclosure of sensitive information contrary to the public interest (e.g. methods of surveillance, names of informants) on the other. As the European Court on Human Rights noted in *Rowe and Davis v United Kingdom*:[86]

> the entitlement to disclosure of relevant evidence is not an absolute right. In any criminal proceedings there may be competing interests, such as national security or the need to protect witnesses at risk of reprisals or keep secret police methods of investigation of crime, which must be weighed against the rights of the accused. In some cases it may be necessary to withhold certain evidence from the defence so as to preserve the fundamental rights of another individual or to safeguard an important public interest.

59. Indeed, as one MP noted during debates on the Serious Organised Crime and Police Bill:[87]

---

[82] See www.cps.gov.uk/legal/section20/JOPI.pdf

[83] In exceptional cases, the prosecution can make an application to withhold disclosure of evidence to a defendant on public interest immunity grounds on an *ex parte* basis, i.e. without the knowledge of the defendant or his lawyers. A special advocate can be appointed to represent the interests of the defendant in relation to disclosure, in order to ensure their right to a fair trial. See *R v H,* para 36: 'in appropriate cases the appointment of special counsel may be a necessary step to ensure that the contentions of the prosecution are tested and the interests of the defendant protected'. See also *Edwards & Lewis v United Kingdom* [2004] ECHR 560.

[84] [2004] UKHL 3 per Lord Bingham at para 17.

[85] Ibid, para 18.

[86] (2000) 30 EHRR 1, para 61

[87] Andrew Mitchell MP, Hansard, HC Debates, 7 Feb 2005, Col 1241

> The withholding of sensitive information is an uncontroversial and unexceptional daily occurrence in the criminal courts. There is a clear public interest in preserving the anonymity of informers; of the identity of a person who has allowed his premises to be used for surveillance, and of anything that would reveal his identity or the location of his premises; of other police observation techniques; and of police and intelligence service reports, manuals and methods. The police order manual, for example, is protected from disclosure. Techniques relating to intercept systems, procedures, technology and methodology fall into the same category.

60. Although it remains for the court to determine for itself which evidence should be disclosed to a defendant in order to secure a fair trial,[88] it is in our view inconceivable that a court would ever conclude that the interests of justice required details of surveillance or interception capabilities to be disclosed. Even were it to do so, however, it would still be open to the Crown to withdraw the prosecution and thereby prevent the sensitive material from being disclosed to the defendant.

61. Indeed, there is no requirement on the prosecution to introduce intercept material into evidence if it does not wish to do so, including those situations where it is feared that its use may inadvertently reveal too much about interception capabilities in the circumstances of a particular case. The decision not to introduce intercept evidence in a particular case, however, should be a matter of judgment for prosecutors. It is impossible to see how such a hypothetical case could be used to justify the existing absolute prohibition on intercept evidence in UK law.

No evidence that PII principles have failed to protect interception capabilities in other jurisdictions

62. Thirdly, in those common law countries where intercept evidence is used regularly in adversarial criminal proceedings, there is no evidence that PII principles have failed to protect either interception capabilities or other methods of covert surveillance.[89] Indeed, given the strength of its concern that use of intercept evidence would lead to criminals and terrorists becoming educated about methods of interception, it is striking that the government has been unable to point to any decline in the value of intercept evidence in those jurisdictions where it is used. On the contrary, prosecutors in other jurisdictions testify to the continuing utility of

---

[88] *R v H*, n84 above, para 37: 'There will be very few cases indeed in which some measure of disclosure to the defence will not be possible, even if this is confined to the fact that an ex parte application is to be made. If even that information is withheld and if the material to be withheld is of significant help to the defendant, there must be a very serious question whether the prosecution should proceed, since special counsel, even if appointed, cannot then receive any instructions from the defence at all'.

[89] See Part 3 below.

intercept evidence. As the Australian federal Director of Public Prosecutions, Damian Bugg QC, noted in 2005:[90]

> We rarely now have a drug importation prosecution that does not have telephone intercept evidence in it. I can think of any number of prosecutions where we would have real difficulty in prosecuting without it – we just would not get the evidence.

Again, there is no evidence that use of intercept evidence in Australia and elsewhere has led to a disclosure of interception capabilities, increased the difficulties of interception operations, or otherwise diluted the value of interception as a tool in the fight against serious organised crime and terrorism.

Intercept evidence would harm relationship between police and intelligence services

63. A frequent governmental argument against the use of intercept evidence in UK courts is the concern that it would lead to a reduction of cooperation between between the intelligence services and the police. In debates on the Serious Organised Crime and Policing Bill, a Home Office Minister Caroline Flint MP explained to Parliament:[91]

> The fact is that we already use intercept evidence to convict criminals, and *without prejudicing the close relationship between our intelligence services and the police*. Indeed, no other country has such a close relationship …

64. At first glance, it is difficult to understand why allowing the use of intercept material as evidence should have any bearing on the working relationship between different agencies. However, in debates on the Terrorism Bill, the Home Office Minister Baroness Scotland QC similarly spoke of the need to protect the 'relationship between intelligence and law enforcement agencies' and ventured that allowing intercept evidence:[92]

---

[90] See n72 above.

[91] Hansard, HC Debates, 7 Feb 2005, Col 1241, emphasis added. See also See also Home Office Minister Hazel Blears MP told the House Hansard, HC Debates, 8 Feb 2005 : Col 1423, emphasis added: 'We have a unique system of *very close co-operation, and I am worried that we would jeopardise it* if we used intercept as evidence'. See also Charles Clarke: Evidence to Home Affairs Committee, HC 321, 8 February 2005, Q15, emphasis added. 'the level of collaboration between law enforcement and intelligence in this country is *uniquely strong*'. Baroness Ramsay of Cartvale, Hansard, HL Debates, 13 December 2005 : Column 1229, emphasis added: 'we have a *uniquely close, interwoven relationship* between our intelligence and security services and our law enforcement agencies. It is therefore much more difficult to disentangle the various contributions of intercept material.'

[92] Hansard, HL Debates, 13 December 2005, Col 1236.

would lead to a reduction in co-operation, in the options available to criminal investigation and in its effectiveness as an intelligence tool and ultimately as an evidential tool.

65. At its root, therefore, the government's concern appears to be that allowing intercept evidence may lead one government agency or public body to refuse to cooperate or share vital information with another. We find such an explanation surprising, to say the least. Whatever the complexities of the working relationship, the suggestion that intercept evidence could lead to an increase in inter-agency tension seems to us a poor argument against allowing its use in court. Similarly, even if such tensions did arise, we do not think it credible that any government would ever permit them to compromise the fight against serious crime and terrorism.

66. In any event, we note that the concerns expressed by government do not appear to be shared by several senior police officers - persons one would assume to be intimately familiar with the 'uniquely close' relationship.[93] As Sir Ian Blair, Metropolitan Police Commissioner, told the Daily Telegraph in February 2005:[94]

> I have long been in favour of intercept evidence being used in court. The court can then weigh it up. At the moment nobody can test it.

67. Nor is it clear that the relationship between intelligence services and law enforcement in the UK is as unique as supposed. In a paper delivered at the JUSTICE/Sweet & Maxwell Conference on Counter-Terrorism and Human Rights in June 2005, a senior lawyer from the Crown Prosecution Service noted:[95]

> [I]t is clear that the relationships between the National Security Agency and the US Department of Justice and between the Australia Security Intelligence Organisation and the various law enforcement agencies in Australia [two countries in which intercept evidence is admissible] are now much closer than they were. *A suggestion that the relationship between the intelligence agencies and law enforcement in the UK is unique in terms of the information flows between them is now more difficult to sustain*.

---

[93] See Appendix.

[94] 'Lift phone tap ban in terror trials, says new Met chief' by Rachel Sylvester, Daily Telegraph, 5 February 2005.

[95] Kingsley Hyland, 'Intercept as Evidence', paper delivered at the JUSTICE/Sweet & Maxwell Conference on Counter-Terrorism and Human Rights, 26 June 2005.

Intercept evidence would hamper ability to adapt to rapid changes in communications technology

68. Another argument made against allowing intercept evidence is the claim that the current rapid pace of change in communications technology is likely to render obsolete any legal framework established to permit its use, and even compromise the ability of law enforcement and intelligence services to intercept new kinds of communication. The Home Secretary in 2005 supported his argument against intercept evidence by noting the 'major changes expected in communications technologies over the next few years'.[96] Similarly, Baroness Scotland argued:[97]

> It does not make sense to change our system just as technology is changing and before we know what that means for how interception is regulated and deployed in future …. Over the next few years, the world of communications technology is likely to change very significantly in lots of ways. Terms such as 'wiretap evidence' will soon be as redundant as talk of telephone operators and switchboards is today. They will be replaced by technologies such as Voice over Internet Protocol (VoIP), where the human voice is broken up into many signals transmitted across a variety of different routes before being brought together again on delivery, rather than being carried over a single line.

69. That communications technology is currently undergoing a period of rapid change is an undeniable fact. We also accept that these changes pose a serious challenge to police and intelligence services carrying out lawful interceptions.[98] As an argument against the *admissibility* of intercept material as evidence, however, the government's reasoning is seriously flawed.

70. The first and most obvious point is that interception of communications is *already* subject to legal regulation under Part I of RIPA. Therefore, the challenges posed by changes in communication technology are those that the current legal framework is bound to confront in any event, regardless of whether intercept evidence is made admissible or not. This is because Article 8 of the European Convention on Human Rights requires that any interference with private communications must be made 'in accordance with the law'. Any attempt to intercept a communication that did not fall within the existing framework would likely fall foul of

---

[96] Written ministerial statement on intercept evidence, 26 Jan 2005, Col 19WS.

[97] Hansard, HL Debates, 13 December 2005 : Column 1236.

[98] However, the argument from technological change does not apply to all areas of intercepted communications. For instance, Part I of RIPA applies not only to the interception of telecommunication systems but also to intercepted letters sent via post – a means of communication whose essential features have not changed substantially in over 400 years.

the minimum requirements of legality.[99] The argument that intercept evidence would require legislation giving rise to excessive rigidity is therefore a red herring: interception itself requires legislation in order to remain lawful. Any change in communications technology that fell outside the current framework would be need to be legislated for in any case.

71. Indeed, it is evident that the requirements of legality have been the engine behind the existing statutory framework for intercepting communications: the 1984 judgment of the European Court of Human Rights in *Malone v United Kingdom*[100] that the lack of statutory framework for interceptions breached Article 8 ECHR led to the Interception of Communication Act 1985. Similarly, the 1997 judgment of the Court in *Halford v United Kingdom*[101] that the lack of regulation over intercepting communications on internal networks under the 1985 Act breached Article 8 ECHR led to the Regulation of Investigatory Powers Act 2000.

72. Secondly, there is nothing in the current legal framework that stipulates the particular *method* of interception. Therefore, so long as the communication falls within the terms of Part I of RIPA, the evidential use of intercept material would make no difference to the ability of police and intelligence services to develop new and increasingly sophisticated means of interception.

73. Thirdly, we are confident that, in the event that new methods of communication fall outside the existing legal framework, they can be addressed by way of prompt amendment and flexible legislative drafting. The interception of communications is far from the only area of law that is affected by rapid technological change (see e.g. intellectual property, data protection, telecommunications in general). We have not heard it suggested that the government should avoid regulating other areas for fear of hampering the effectiveness of police and intelligence services.

74. Indeed, the continuing failure of government to develop techniques for using intercept material as evidence in the modern digital age may prove more deleterious to police and intelligence efforts than legislating for its use. As the Foundation for Information Policy Research noted in 1999, the very fast pace of technical developments in the field of digital intercepts was a positive argument in favour of allowing intercept evidence, rather than continuing to prohibit its use:[102]

---

[99] See section on the use of intercept evidence under the European Convention on Human Rights, paras 108-114 below.

[100] See note 60 above.

[101] See note 64 above.

[102] Foundation for Information Policy Research, *Interception of Communications in the United Kingdom: A response to the Home Office Consultation Paper* (16 August 1999).

> Unless law-enforcement takes the plunge, and begins to develop techniques for forensic acquisition and competent presentation of intercept evidence, it will be left hopelessly far behind.

Intercept evidence would increase burden on intelligences services, police and prosecutors

75. Opponents of intercept evidence argue that allowing its use would inevitably lead to the police and intelligence services having to devote resources to transcribing and retaining intercept material for use at trial, as well as putting pressure on prosecutors and courts dealing with requests for disclosure from defendants.[103] As the Joint Committee on Human Rights noted in its August 2006 report:[104]

> The CPS's perception was that the main objection of the security services [to allowing intercept evidence] was the purely practical one of resources, given the large volume of material to be recorded, transcribed and kept in case it was ordered to be disclosed. This was seen as potentially very time consuming and expensive. The security services would prefer to devote those resources to ensuring that technological developments, such as the advent of internet telephony, did not diminish their capacity to capture information.

76. Other opponents of intercept evidence similarly paint a lurid picture:[105]

> [Intercept evidence would impose] enormous burdens of transcribing and preserving all related interception material if it is to be available for court evidence. That would certainly mean a considerable diminution of product from the services concerned, because of the sheer volume of what would have to be processed and kept

77. At the outset, we think it is sensible to concede that allowing intercept evidence will result in an increased burden on police, prosecutors and the intelligence services in terms of

---

[103] See e.g. Lord Dubs, Minister in the Northern Ireland Office, HL Debates, 26 Mar 1998 : Column 1362: 'the use of intercept material would result in pressure for increased disclosure by the prosecution'.

[104] JCHR, *Counter-Terrorism Policy and Human Rights: Prosecution and Pre-charge Detention*, (HL 240/HC 1576: 1 August 2006), para 100.

[105] Baroness Ramsey of Cartvale, Hansard, HL Debates, 18 November 2005 : Column 1306. See also e.g. Lord Robertson of Port Ellen, Hansard HL Debates, 18 Nov 2005 : Column 1311: 'If one element of evidence is put into court, it will be simply a matter of time, logic or even fairness that all the intercepted information is placed outside the protected world where it had previously resided … Depending on the discretion of the judge—at the end of the day, that is what we would be depending on—the defence can range far and wide, as it has done in the past, and compromise material that should not be compromised.'

transcribing and retaining intercept material with a view to future criminal proceedings.[106] However, we consider the estimates above – including the suggestion that *all* intercept material would have to be transcribed – to be highly exaggerated. To the extent that using intercept material as evidence would pose challenges to the police and the intelligence services, we believe that these are hardly insurmountable – indeed, they have been met in every common law jurisdiction in which intercept is used – and that the benefits considerably outweigh the costs.

78. In particular, we consider that fears of defence lawyers mounting extensive fishing expeditions in search of undisclosed material to be unfounded, so long as prosecutors and courts perform their respective roles with diligence. As Lord Bingham noted in *R v H,*[107] 'if material does not weaken the prosecution case or strengthen that of the defendant, there is no requirement to disclose it':[108]

> The trial process is not well served if the defence are permitted to make general and unspecified allegations and then seek far-reaching disclosure in the hope that material may turn up to make them good. *Neutral material or material damaging to the defendant need not be disclosed and should not be brought to the attention of the court.* Only in truly borderline cases should the prosecution seek a judicial ruling on the disclosability of material in its hands.

79. Lastly, we note that concerns about the logistical burden were also dismissed by Assistant Commissioner Andy Hayman in his evidence to the Home Affairs Committee:[109]

> The next point which I had reservations about was the true logistics about transcribing [intercept] material, where you could go into reams of material. Again, that is a fairly moot point now, given that *you can be very selective about the things you are going to transcribe if you are very precise on your investigation and focused*. I think I am moving, as I know ACPO is, to a conclusion that in a selected number of cases, not

---

[106] See e.g. the 1999 Consultation paper, n31 above, para 8.8: 'any arrangements which make intercept material available to one or both parties would have to be both practical and affordable'.

[107] [2004] UKHL 3.

[108] Ibid at para 35. See also the Director of Public Prosecutions, Ken Macdonald QC, evidence to JCHR, 19 May 2004 Q51: '[W]e disclose to the defence all the material upon which we intend to rely in the trial. We also disclose to them any material which, in our judgment, undermines our case or supports their case. So if we have material that we do not intend to rely on but which does not undermine our case or support their case, it is not disclosable under statute. The reality of the situation is that one would be considering material which was material that we would be intending to rely on, I suppose, otherwise it is of no interest to us. Equally, if we are not intending to rely on it and it does not help the defence or undermine our case, it is of no interest to the defence either. It is simply irrelevant to any issue in the case'.

[109] Evidence to the Home Affairs Committee, Q244, 28 February 2006, emphasis added.

> just for terrorism but also for serious crime, it would be useful. I think also it does make us look a little bit foolish that everywhere else in the world is using it to good effect.

Intercept evidence is unsuited to adversarial criminal proceedings

80. Perhaps the most inaccurate argument against intercept evidence has been the widely-repeated claim that intercept evidence is used primarily in inquisitorial legal systems and is therefore ill-suited to adversarial legal systems such as the UK. As the following exchange between the Home Affairs Committee and the then-Home Secretary shows:[110]

> *Mrs Curtis-Thomas:* Home Secretary, if intercept evidence is accepted in other countries where there are robust court systems and democratic accountability then why not here?
>
> *Mr Clarke:* Essentially because our legal system is entirely different. The fact is the whole nature of the judicial system, for example in France or Spain or wherever, is entirely different from our regime first and foremost, so the role of judges, and in particular *juge d'instruction*, in their systems is different from ours.

81. A member of the Intelligence and Security Committee, Baroness Ramsay of Cartvale, similarly informed Parliament:[111]

> our adversarial legal system, where defence counsel can roam widely at the discretion of the judge, produces in the case of intercept material an unacceptable risk of exposure …. Countries whose legal systems have investigative judges or magistrates can manage to handle sensitive material without the risks that would be involved in using such material in a British court.

82. Nor are these beliefs confined to Parliament and the Executive branches. In his 2003 review of criminal investigations and prosecutions conducted by Customs & Excise, Mr Justice Butterfield referred the use of intercept material as evidence in criminal proceedings in Holland but noted that 'the inquisitorial investigation and trial process in Holland is however very different to accusatorial system operating in the United Kingdom'[112] and gave his view that:[113]

---

[110] HC 321, 8 February 2005, Q15.

[111] Hansard, HL Debates, 13 December 2005 : Column 1229.

[112] Butterfield J, *Review of criminal investigations and prosecutions conducted by HM Customs and Excise* (July 2003), para 12.103.

[113] Ibid, para 12.107.

> For so long as our criminal system remains accusatorial I am of the view that there is no realistic scope for the use of intercept material for evidential purposes in criminal proceedings.

83. Such official explanations no doubt contribute to such popular accounts such as that given by one former Cabinet Minister:[114]

> I was sternly told the British system of justice is quite different from that which guides the courts in countries where phone-tap evidence is allowed. Our trials are adversarial. The barrister defending the terrorist suspect would demand to know how the intercepts had been obtained, who had obtained them and by whom they had been sent. The result, it was claimed, would be the exposure of dangerous details about the activities of MI5 and MI6. Foreign governments might be offended. Brave men's lives would be at risk.

84. As we set out in Part 3 of this report, intercept evidence has been long been admissible in criminal proceedings in Australia, Canada, New Zealand, South Africa and the United States. These are all jurisdictions that operate adversarial criminal proceedings, and have inherited principles of evidence and criminal procedure from the English common law. As we have already noted,[115] there is no evidence that these jurisdictions have experienced any of the difficulties alleged above due to their lack of inquisitorial proceedings. We therefore are at a loss to understand why the inquisitorial claim should have been so widely repeated by government sources and find it disturbing that public debate over such an important issue can be confounded by such misinformation.

Intercept evidence unlikely to show guilt

85. In the run-up to the Prevention of Terrorism Bill 2005, the government produced background briefing papers for MPs and Peers. One of the background papers claimed:[116]

> The usefulness of intercept as an evidential resource, as opposed to an intelligence one - showing who is talking to whom, where they are located, and sometimes clues to what they are discussing - is … severely limited by the sophistication of the terrorists who rarely incriminate themselves over the telephone or fax.

---

[114] Roy Hattersley, 'Terrorism, marmalade and MI5', *The Guardian*, 7 February 2005.

[115] See para 62 above.

[116] *International Terrorism: Reconciling Liberty And Security - The Government's Strategy To Reduce The Threat* (Home Office, 22 February 2005).

86. We readily accept that intercept evidence is not a silver bullet: no doubt the intercepted conversations of suspected criminals and terrorists often fails to yield useful material. But the problem of suspects communicating using code words or other guarded language is hardly a problem unique to intercept evidence. The same challenge is presented by evidence gained from other forms of covert surveillance – such as bugs or concealed microphones worn by informants – all of which are admissible in criminal proceedings. Indeed, a similar challenge exists in relation to *any* evidence in criminal proceedings which requires some form of interpretation in order to explain it to a jury. Just as juries are able to consider DNA evidence without being geneticists or forensic evidence without being scientists, it seems implausible that intercept material is only useful in the hands of an intelligence expert.

87. More generally, it is naïve to suppose that intercept evidence could only be useful where it records suspects openly admitting their guilt: just as interceptions may be useful for intelligence purposes, they may also present compelling *circumstantial* evidence that a crime has been, or is about to be, committed. As the Australian federal Director of Public Prosecutions explained to the Guardian newspaper:[117]

> You can have what you might call a circumstantial case where three people are seen having coffee together three times a day and that activity has intensified over a couple of weeks leading up to the arrival of a package or container in Australia. And then they undertake connected activities. You might, on behalf of one of those people, argue that it was an innocent association and you can't quite link them to the transaction. You just have to have these identifiable and suspicious acts of association …. When you fill in the gaps with telephone intercepts, this gets the police inside the network. When you show a jury these isolated physical acts which you say are, on the surface, suspicious and then fill in the landscape, *it strengthens your case substantially*.

88. FBI Director Louis Freeh similarly cited the importance of intercept evidence in building a case: [118]

> Because national and international drug chieftains and local drug 'kingpins' do not generally participate directly in drug buys or shipments, *electronic surveillance frequently supplies the only direct and persuasive evidence that will support a criminal conviction of these drug 'kingpins'.*

---

[117] See Clare Dyer, n72 above, emphasis added.

[118] Statement of Louis Freeh, FBI Director, to the Federal Communications Commission, 27 January 1999, para 18.

Arguments for lifting the ban

Intercept evidence would increase likelihood of convictions for terrorism offences

89. The best-known argument in favour of allowing intercepted communications as evidence in criminal proceedings is that they are likely to contain material which is both relevant and highly probative to the issue of whether the accused committed the offence in question. Given the complexity of serious organised crime and terrorism, they are particularly likely to be useful in prosecuting those offences.

90. This argument is often resisted by government, however. Reporting on the conclusion of an internal government review in February 2005, the Home Secretary said that 'evidential use of intercept would be likely to help secure a modest increase in convictions of some serious criminals but not terrorists'.[119] Since the review is itself classified, however, we are not in a position to analyse its evidence or reasoning. More generally, because the great majority of intercept material remains classified, the argument in favour of using intercept relies heavily on the views of those involved in the detection, investigation and prosecution of serious crime and terrorism in the UK, as well as the publicly-available evidence concerning the use of intercept evidence in other jurisdictions.

91. First, the government's claim that intercept evidence is unlikely to assist in prosecuting terrorism cases in the UK seems difficult to reconcile with the use of intercept evidence in other jurisdictions. In his 1996 report, for instance, Lord Lloyd reported that, in France, 'some 80% of the evidence against those suspected in the 1995 bombings is derived from intercept' and that 'intercept evidence has proved very valuable in terrorist cases' there.[120] Similarly, in respect of US prosecutions, FBI Director Louis Freeh stated in 1999:[121]

> Law enforcement agencies at all levels of government have uniformly found electronic surveillance to be one of the most important – if not *the* most important – sophisticated investigative tools available to them in the prevention, investigation and prosecution of many serious types of crime. This tool has been critical in fighting terrorism, organized crime, kidnapping, public corruption, fraud and violent crime, and in saving numerous innocent lives. In many of these cases, the criminal activity under investigation could never have been detected, prevented, investigated or successfully

---

[119] Written ministerial statement on intercept evidence, 26 Jan 2005, Col 18WS.

[120] Lloyd report, n33 above, para 7.10

[121] Statement of Louis Freeh, n120 above, para 10, emphasis in original. For details of the use of intercepts in US law enforcement, see *Report of the Administrative Director of the United States Courts on Applications for Authorizing or Approving the Interception of Wire, Oral or Electronic Communications, 2005*: www.uscourts.gov/wiretap05/WTText.pdf

prosecuted without the use of evidence derived from court-authorised electronic surveillance.

92. Similarly, the annual report of the Canadian federal government on the use of electronic surveillance released in September 2006 noted that:[122]

> *The use of electronic surveillance often provides strong evidence against those accused of being involved in illegal activities, increasing the likelihood of conviction.* The prosecution of such offenders increases public confidence in the criminal justice system and contributes to public safety by holding such persons responsible for their actions.

93. In an amicus brief lodged in 2005, former US Attorney General Janet Reno gave the following examples of terrorism cases prosecuted in the US since 9/11 involving intercept evidence:[123]

- Iyman Faris pleaded guilty to providing material support for terrorism. Faris visited an al Qaeda training camp in Afghanistan and investigated the destruction of bridges in the United States by severing their suspension cables. The government *secured evidence through* physical and *electronic surveillance* and a search of his residence. After his arrest Faris cooperated with investigators, leading to the indictment of Nuradin Abdi for plotting to blow up a Columbus, Ohio shopping mall.

- Several members of a terrorist cell in Portland, Oregon were indicted on conspiracy, material support, and firearms charges. One of the defendants pleaded guilty and testified against the others, securing guilty pleas from them. Six of the men had attempted to travel to Afghanistan to assist the Taliban. The government used *electronic surveillance* and the authorities of the USA PATRIOT Act *to gather evidence in the case*.

- Six residents of Lackawanna, New York pleaded guilty to charges arising from their travel to Afghanistan and attendance at al Qaeda training camps. *The evidence against them was gathered from electronic surveillance.* They agreed to cooperate with government investigations of terrorist activities.

---

[122] In particular, 12 authorisations for interception between 2004-2005 were given for specific terrorist offences - see Table 4 (offences in respect of which authorizations were given, specifying the number of authorizations given in respect of each of those offences), ibid, pp 8-9.

[123] Brief of Janet Reno and others as Amicus Curiae in *Padilla v Commander, Consolidated Naval Brig*, (No 05-6396), 14 June 2005, pp 23-24, emphasis added. P2 of the brief makes clear that 'electronic surveillance' is the equivalent term to telecommunication interceptions.

- Sami Al-Arian, a university professor, and seven others were indicted for conspiring to finance terrorist attacks. The Justice Department reports that the evidence against Al-Arian was *gleaned from extensive FISA wiretaps, which could be used in the criminal case because of the new procedures enacted by the USA PATRIOT Act*.

94. Given the significant use of intercept evidence in terrorism prosecutions in other common law countries, the strong links between terrorist activity and serious organised crime,[124] and the international nature of terrorism itself,[125]it would seem suprising that intercepted communications of suspected terrorists in the UK are somehow alone in failing to provide relevant material for prosecutors.

95. Secondly, the claim that intercept evidence is unlikely to assist in prosecuting terrorism cases in the UK seems difficult to reconcile with the statements of senior police and prosecutors, judges and others familiar with the classified material.[126] In his 1996 review of terrorism legislation, Lord Lloyd reported that:[127]

> It is always difficult to look backwards and point to specific cases in which interception material would have enabled a person to be charged or a conviction obtained. But I have been shown a list of some twenty cases, including four recent cases in which the intercept material would have been of assistance to the prosecution; and I was told of at least one terrorist investigation in which the interception evidence would have provided 'the missing pieces in the jigsaw' and thus enabled a prosecution to be brought.

96. Lord Carlile of Berriew QC, the current statutory reviewer of terrorism legislation, has similarly argued:[128]

---

[124] See e.g. then-Home Secretary Charles Clarke, Hansard, HC Debates, 7 December 2004: 'All nations are considering the interrelationship between serious organised crime and terrorism'. See also Home Office, *Counter-Terrorism Powers: Reconciling Liberty and Security in an Open Society* (Cm 6147: February 2004) at p27: 'much existing legislation aimed at combating organised crime is also helpful in the fight against terrorists who often rely on such methods to finance their activity'.

[125] See e.g. n78 above.

[126] See Appendix.

[127] Lloyd Report, n33 above, para 7.11

[128] Lord Carlile of Berriew QC, *Proposals By Her Majesty's Government For Changes To The Laws Against Terrorism,* 6 October 2005.

> the potential to use intercept evidence should be available. This would not mean that it would have to be used. In a small number of terrorism cases, and probably a larger number of drug-smuggling and money-laundering cases, and possibly in other categories of crime especially with an international dimension, it would help to secure convictions.

97. Lastly, as a matter of simple logic, it seems difficult to reconcile the government's doubts about the utility of intercept material as evidence in terrorism cases with its self-same faith in intercept material to produce reliable intelligence on terror networks.[129] The experience of other jurisdictions shows that intercept material may be made readily intelligible to juries and provide evidence that is highly probative despite being circumstantial.[130]

Intercept evidence would reduce pressure for extended pre-charge detention in terrorism cases

98. As noted above, evidential difficulties in terrorism cases were widely cited as the reason for the extension of the maximum period of pre-charge detention to 28 days under the Terrorism Act 2006.[131] Although intercept material is often used as the grounds for arrest under section 41 of the Terrorism Act 2000, it cannot be used as the basis for preferring criminal charges for terrorist offences because it is inadmissible as evidence in legal proceedings. It therefore stands to reason that, were intercept material admissible as evidence, it could be used to charge those suspected of terrorist offences within the original 14 day maximum detention period.[132] However, the then-Home Secretary Charles Clarke rejected this argument in his memorandum to the Home Affairs Committee:[133]

> Even if such a change could be made it would not apply in every case and could not therefore, of itself, remove the need for an extended pre-charge detention period.

99. Although we readily accept that intercept evidence is not a silver bullet, the Home Secretary's reply appears wholly to miss the point. Regardless of whether intercept evidence would by itself obviate the need for extended pre-charge detention in *all* terrorism cases, it is clear that it

---

129 Conor Gearty, 'Short Cuts', *London Review of Books*, 17 March 2005: 'The government's reluctance to allow intercept evidence to be used in court to procure conviction of terrorist suspects seems mysterious and self-defeating: why deny yourself such a key weapon in the 'war against terrorism', especially if there are 'several hundred' terrorists already in the country, as the prime minister has recently claimed?'

130 See paras 87 and 88 above and Part 3 below.

131 Section 23 of the Terrorism Act 2006.

132 Schedule 8, Terrorism Act 2000, as amended by section 306 of the Criminal Justice Act 2003.

133 Memorandum of the Secretary of State for the Home Department to the Home Affairs Committee, *Terrorism Detention Powers* (4th Report, HC 910: 3 July 2006), Ev 101.

would make a significant difference in *every* case where intercept material was the basis of reasonable suspicion of involvement in terrorism in the first place. Indeed, in the scenario posed by the Chief Constable of Greater Manchester,[134] it would allow the suspect to be arrested and charged without the need for extended pre-charge detention:

> If you have information from an informer, if you have technical surveillance evidence, if you have intercept evidence, there is a whole series of things which actually says, 'This group of people or this individual are involved in the preparation for some form of act of terrorism', then we will arrest.

Intercept evidence would increase fairness of trials

100. Earlier we argued that intercept evidence would increase the likelihood of convictions in terrorism cases. However, there is a separate reason for favouring the use of intercept evidence and that is that it would increase the fairness of criminal proceedings as a whole: to both the prosecution and the defence. This is not as contradictory as it might appear because, as a matter of logic, the more relevant evidence that is admissible, the more likely it is that the jury will arrive at the correct conclusion. By contrast, under the current statutory framework, intercept material is inadmissible as evidence, regardless of whether it is favourable to the prosecution or the defence.

101. The fairness of allowing intercept evidence was considered by the House of Lords in the case of *R v P*,[135] in which the defendants appealed against their conviction on the basis that the prosecution's use of foreign intercept evidence was contrary to their right to a fair trial under both English law and Article 6 of the European Convention on Human Rights. The Law Lords unanimously rejected the appeal, holding that the evidence was not unfair and that there was no basis in public policy for excluding foreign intercept evidence.[136] On the contrary, Lord Hobhouse noted, the right to a fair trial *positively required* the most relevant evidence to be used:[137]

> The tape recordings and transcripts (about the accuracy of which, be it said, there is no dispute) will be the *best evidence* of what was said. *The fairness of the trial of these defendants requires that the evidence be admissible.*

---

[134] Evidence to the Home Affairs Committee, 8 July 2004, Q59.

[135] (2001) 2 All ER 58.

[136] See ibid, per Lord Hobhouse at 73: 'The law of country A under which these intercepts were made does not treat secrecy as paramount; it permits, subject to judicial supervision, the use of intercepts in evidence. There is no basis for the argument that there is a rule of English public policy which makes this evidence, which is admissible in country A, inadmissible in England'.

Intercept evidence already used in criminal proceedings

102. The various arguments mounted against intercept evidence in criminal trials are significantly undermined by the fact that (i) intercept evidence is already admissible in a number of circumstances; [138] and (ii) all other kinds of covert surveillance evidence are admissible.[139] For instance, an intercept of a telephone conversation is admissible if:

- it has been recorded by one party;[140]
- it has been recorded by a covert listening device, rather than a direct intercept of the telecommunication network;[141]
- it is made to or from a prison (see e.g. Ian Huntley) or a secure mental health facility;[142] or
- it is recorded outside the UK.[143]

---

[137] Ibid, per Lord Hobhouse at 74.

[138] See e.g. Guy Mansfield QC, Chair of the Bar Council of England and Wales, statement 'Intercept evidence – no legal or operational problem with using it in court', 18 February 2005: 'The current law is illogical. Broadly speaking, telephone intercept evidence cannot be used. However, telephone intercepts lawfully obtained in foreign jurisdictions are admissible in English courts. A tape recording of a telephone conversation made by one of the participants is admissible. Conversations recorded from a bug legally planted in premises used by drug dealers are admissible, and such conversations can include what is said by a suspect into the telephone'; see also Andrew Mitchell MP, Hansard, HC Debates, 7 Feb 2005, Col 1238: 'there are already eclectic and disparate cases in which intercept evidence is used in criminal courts, albeit as an exception to the general rule, and there has not been any damage to police or intelligence service operational capabilities and methodology.'

[139] See also Lord Thomas of Gresford, HL Debates, 18 Nov 2005 : Column 1328: 'Intercept evidence is not admissible, but directed or intrusive surveillance or the use of covert human intelligence under Part 2 of the Regulation of Investigatory Powers Act 2000, can be. So, for example, there is no problem about a member of the security services breaking into somebody's home and planting a bug there or for the product of that particular piece of covert surveillance being used in court. If a person's car is bugged, there is no problem in producing a record of the conversations that take place within the car. So, on the one hand, there is total prohibition on intercept evidence, and, on the other, you can use foreign intercept evidence and the product of surveillance freely in the courts of this country'.

[140] Section 48(4) RIPA.

[141] A recording of a person speaking into a mobile phone is not an interception of a communication 'within the course of its transmission' within the meaning of section 2(2) of RIPA: see *R v E* [2004] EWCA Crim 1243. See also *R v Smart and Beard* [2002] EWCA Crim 772 (DAT recordings of a suspect speaking into a telephone was not an 'interception' within the meaning of s1(1) of the 1985 Act).

[142] Section 4(4) RIPA. See also *R v Allan and others* [2001] EWCA Crim 1027: evidence of telephone calls via a prison phone network admissible because not within s1(1) of the 1985 Act.

[143] Section 4(1) RIPA. See also *R v P*, n137 above.

103. For example, intercept evidence of telephone calls between Ian Huntley, Maxine Carr and Huntley's mother was used to help convict Huntley of the Soham murders in December 2003. The jury heard recordings and read transcripts of taped conversations of calls made by Huntley from Woodhill Prison, and calls by Maxine Carr from Holloway prison.[144] The intercepts were admissible because they took place under one of the exceptions under section 4(4) of RIPA where an intercept warrant is not required. In many other cases, intercept evidence admissible under one of the above exceptions has been used to convict suspects accused of serious crimes. Evidence from other forms of covert surveillance have similarly been widely used in securing convictions. Again, there is no bar to the admissibility of evidence gained from:

- a covert listening device (i.e. a bug) in someone's home, office or vehicle;[145]
- a concealed microphone worn by an informant;[146] or
- external surveillance of a home or office, including via video camera.[147]

104. If the arguments concerning fear over disclosure of intercept evidence capacity or the inability of PII to protect against disclosure were credible, one would expect to find the same arguments mounted against the use of evidence from other kinds of covert surveillance, such as bugging, informant evidence or evidence from covert video surveillance. As the Hong Kong Law Reform Commission observed in March 2006, 'there is no basis for the assertion that surveillance capability is more, or less, well-known than that in respect of interception'.[148]

---

[144] See e.g. BBC Online, 'Huntley set fire to girls' bodies', 28 November 2003, www.bbc.co.uk/1/hi/uk/3246118.stm

[145] Part II of RIPA governs directed and intrusive surveillance other than interceptions. For examples of admissible evidence from bugs see *R v Allsop and others* [2005] EWCA Crim 703; *R v E*, n143 above (DAT recording from bug in car).

[146] See e.g. *Code of Practice: Covert Human Intelligence Sources* (Home Office), para 4.41: 'a source, whether or not wearing or carrying a surveillance device, and invited into residential premises or a private vehicle, does not require additional authorisation [under Part II of RIPA] to record any activity taking place inside those premises or vehicle which take place in his presence'.

[147] See e.g. *R v Rosenberg* [2006] EWCA Crim 6.

[148] Hong Kong Law Reform Commission, *Privacy: the Regulation of Covert Surveillance,* n22 above, para 5.60. See also the remarks of La Forest J in the Canadian Supreme Court case of *R v Duarte* [1990] 1 SCR 30: 'I am unable to see any logic to this distinction between third party electronic surveillance and participant surveillance. The question whether unauthorized electronic surveillance of private communications violates a reasonable expectation of privacy cannot, in my view, turn on the location of the hidden microphone. Whether the microphone is hidden in the wall or concealed on the body of a participant to the conversation, the assessment whether the surreptitious recording trenches on a reasonable expectation of privacy must turn on whether the person whose words were recorded spoke in circumstances in which it was reasonable for that person to expect that his or her words would only be heard by the persons he or she was addressing. As I see it, where persons have reasonable grounds to believe their communications are private communications in the sense

105. Were it the case that UK courts were ill-equipped to handle intercept evidence, therefore, one would expect the government to be able to demonstrate this by reference to the existing UK cases in which intercept evidence or other covert surveillance evidence has already been used. The failure of the government to point to such cases suggests that the arguments against the general use of intercept evidence have been significantly overplayed.

---

defined above, the unauthorized surreptitious electronic recording of those communications cannot fail to be perceived as an intrusion on a reasonable expectation of privacy'.

PART 3

106. In February 2005, the then-Home Office Minister Hazel Blears told Parliament:[149]

> Our adversarial system complies with the European convention on human rights and contains a number of hurdles that make it very difficult to use intercept as evidence.

107. In fact, there is nothing in the European Convention on Human Rights that prevents the use of intercept evidence, nor does the adversarial system pose any serious obstacles to its use. The first section in this Part examines the relevant law under the Convention. The second section examines the use of intercept evidence in seven other common law jurisdictions: Australia, Canada, Hong Kong, Ireland, New Zealand, United States and South Africa.

The use of intercept evidence under the European Convention on Human Rights

108. In a series of cases, the European Court of Human Rights has considered a variety of objections to the use of intercepted communications as evidence in criminal proceedings: chiefly under Article 6, the right to a fair trial, and Article 8, the right to respect for privacy. In each case, the Court has made clear that there is, in principle, no bar on the use of intercept evidence under the European Convention on Human Rights.

109. In *Malone v United Kingdom*,[150] the applicant complained that warrants by the Home Secretary authorising police to intercept his telephone conversations breached his right to respect for privacy under Article 8. In an earlier ruling by the English Court of Appeal, Sir Robert Megarry VC had held that interceptions were lawful but observed that 'telephone tapping is a subject which cries out for legislation'.[151] The European Court of Human Rights went further and concluded that the lack of legislation governing intercepts was itself a breach of Article 8 because it failed clearly to identify 'the scope and manner of exercise of the relevant discretion conferred on the public authorities' and therefore 'the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society is lacking'.[152] However, the Strasbourg Court was also careful to note that:[153]

---

[149] Hansard, HC Debates, 8 February 2005 : Column 1423

[150] *Malone v United Kingdom* (1984) 7 EHRR 14

[151] *Malone v Metropolitan Police Commissioner*, [1979] 2 All ER 629 at 649.

[152] Note 156 above, para 79.

[153] Ibid, para 81.

the existence of some law granting powers of interception of communications to aid the police in their function of investigating and detecting crime may be 'necessary in a democratic society ... for the prevention of disorder or crime', within the meaning of Article 8(2),

The Court also noted that covert interception of communications by law enforcement or intelligence services could 'only be regarded as 'necessary in a democratic society' if the particular system of secret surveillance adopted contains adequate guarantees against abuse'.[154]

110. In *Schenk v Switzerland,*[155] the applicant objected to the fact that he had been convicted of attempted murder partly on the basis of an unauthorised interception of his telephone calls by the Swiss authorities. He argued that the use of unlawfully obtained evidence rendered his trial unfair, contrary to Article 6. However, the European Court of Human Rights rejected his argument. It found that even though the interception was unlawful under Swiss law, the rules governing the admissibility of evidence were a matter for national law and that it could not therefore 'exclude as a matter of principle and in the abstract that unlawfully obtained evidence of this kind may be admissible'.[156]

111. In *Chinoy v United Kingdom*,[157] the applicant complained that his extradition from the UK to the United States on the basis of intercept evidence obtained in France by US customs agents without the knowledge of the French authorities breached his rights to liberty and privacy under Articles 5 and 8 respectively. The European Commission on Human Rights, however ruled that the complaint was inadmissible: the fact that the intercept evidence may have been unlawfully obtained in France did not ultimately determine its admissibility in the UK and it was clear that the UK court found the evidence to be relevant.[158] It was therefore open to the UK court to decide to admit the evidence, notwithstanding the apparently unlawful manner in which it was obtained.[159]

112. The case of *Halford v United Kingdom*[160] raised very similar issues to those of *Malone*. The applicant complained that interception of telephone calls made on an internal phone network breached her right to privacy under Article 8, because the Interception of

---

[154] Ibid.

[155] (1988) 13 EHRR 242.

[156] Ibid, para 46.

[157] Application No. 15199/89, decision of 4 September 1991.

[158] Ibid, para 2.

[159] Ibid, para 2.

[160] (1997) 24 EHRR 523, para 51

Communications Act 1985 only applied to interceptions on public networks. The European Court of Human Rights agreed:[161]

> The Court notes that the 1985 Act does not apply to internal communications systems operated by public authorities … and that there is no other provision in domestic law to regulate interceptions of telephone calls made on such systems ... It cannot therefore be said that the interference was 'in accordance with the law' for the purposes of Article 8(2) of the Convention, since the domestic law did not provide adequate protection to Ms Halford against interferences by the police with her right to respect for her private life and correspondence.

113. Again, the Court noted that the violation in the applicant's case was not the practice of intercepting communications but the failure of the law properly to regulate it:[162]

> In the context of secret measures of surveillance or interception of communications by public authorities, because of the lack of public scrutiny and the risk of misuse of power, *the domestic law must provide some protection to the individual against arbitrary interference with Article 8 rights*. Thus, the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to resort to any such secret measures

114. In *Taylor-Sabori v United Kingdom*,[163] the European Court similarly ruled that police interception of pager messages without statutory authority was a breach of the applicant's right to privacy under Article 8.

---

[161] Ibid, para 51.

[162] Ibid, para 49, emphasis added.

[163] (2003) 36 EHRR 17

The use of intercept evidence in common law jurisdictions

Australia

115. As a federal jurisdiction, the authority to make laws in Australia is divided between the federal government (the Commonwealth of Australia) and the States and Territories (e.g. New South Wales, Victoria, etc). Under the Australian Constitution,[164] both the federal and State governments have concurrent powers in relation to criminal law and policing. However, the authorisation of interceptions of communications by police and intelligence services is largely governed by Federal law, as is their use as evidence in criminal proceedings.

116. The lawful authority to intercept communications is spread across different Acts. In particular, a different regime governs postal interception (the Australian Postal Corporation Act 1989) than that of telecommunications (the Telecommunications (Interception and Access) Act 1979).[165]

Interception of telecommunications

117. The 1979 Telecommunications Act governs all forms of lawful surveillance involving telecommunications, including interceptions. 'Telecommunications' is broadly defined in the Act to include 'communications by means of guided or unguided electromagnetic energy or both':[166] e.g. both telephone calls and emails. However, it does not extend to surveillance of sounds made prior to or following transmission via a telecommunications system,[167] e.g. a recording of a telephone call made by an external microphone.

118. The 1979 Act prohibits interception of communications save as authorised by the Act. In particular, lawful interception is permitted where a warrant is issued and in a limited number of other circumstances.[168] Two types of warrants are available for telecommunications

---

[164] Commonwealth of Australia Constitution Act 1900.

[165] Known as the Telecommunications Act.

[166] Section 5.

[167] Russell G. Smith, *Controlling the Interception of Communications: Law or Technology?* Presented at the Communications Research Forum, Canberra, 2 October 1997.

[168] See sections 7(2)–7(5). The other relevant conditions relate to interceptions in exceptional situations where a warrant cannot be practicably obtained, e.g. where there is a risk of loss of life or serious injury and one of the parties to the communication consents. There are also a number of other exceptions relating to employees of telecommunication companies who need to intercept communications for the purposes of performing their duty or complying with regulations.

interceptions: *national security warrants* issued by the Attorney-General[169] authorising interceptions by the Australian Security Intelligence Organisation ('ASIO') for intelligence purposes;[170] or *law enforcement warrants* issued on application to a judge.[171] The latter type of warrant is only available where the interception is likely to assist in the investigation of a 'serious offence', including acts of terrorism.[172] Moreover, when considering the application for a warrant, the judge must weigh a number of factors including the gravity of the offence under investigation.[173] Amendments in 2002 and 2004 were made specifically to facilitate the use of interceptions for terrorist offences.[174]

119. Although a distinction appears to have been made historically,[175] with the exception of ASIO's intelligence warrants,[176] there is no broader distinction in the legislation between interception by law enforcement for the purposes of gathering intelligence on the one hand and interception for the purposes of gathering evidence on the other. Instead, interception warrants are granted on the basis of whether the interception will assist in investigating a criminal offence.[177]

120. Telecommunication intercepts obtained under the 1979 Act, other than foreign intelligence information, are only admissible as evidence in 'exempt proceedings'.[178] However, 'exempt proceeding' is very broadly defined and includes all crimes punishable by 3 years imprisonment or more.[179] In addition, any intercept used in an exempt proceeding may subsequently be used in any other proceedings.[180]

---

[169] In exceptional cases, the ASIO Director-General of Security can grant an emergency warrant under section 10. These warrants can last up to 48 hours only. In addition, Part II also contains provisions for warrants that cover the collection of foreign intelligence.

[170] See section 9(1)(a)(i)-(ii). These provisions have been criticised as being too broad in scope. For example, the report of the Senate Legal and Constitutional Legislation Committee, on the Telecommunications (Interception) Amendment Bill 2006, of 13 March 2006 notes that the Act now allows interceptions of the communications of innocent third parties.

[171] Alternatively, a law enforcement agency may apply for a warrant to a nominated member of the Administrative Appeals Tribunal. See generally Part 2-5 of the 1979 Act.

[172] Section 5D(1)(d). See Annex A for a full copy of Section 5D.

[173] Section 46(1)(d) and section 46(2)(a)-(f). See Annex A for a list of the relevant factors.

[174] See the *Telecommunications Interception Legislation Amendment Act 2002* and the *Telecommunications Interception Legislation Amendment Act 2004*.

[175] See Simon Bronitt, *Electronic Surveillance, Human Rights and Criminal Justice* [1997] AJHR 10: 'Wiretaps and listening devices were initially restricted to an intelligence-gathering function: the public interest in maintaining the secrecy of covert police activity dictated that tapes or transcripts of intercepted communications could not be tendered as evidence at trial'.

[176] See for example, section 9(1)(b) of the Telecommunications Act and section 27(2)(b) and section 27A(1)(a) of the ASIO Act.

[177] See for example section 46(1)(d) of the Telecommunications Act and section 14(1) of the Surveillance Act.

[178] Sections 74(1), 77 and 143(1)

[179] Section 74(1) and 143(1) and the definition of 'exempt proceedings' in section 5.

[180] Section 75A. This amendment was made in 2006 to overcome the result of a NSW Court of Appeal decision, *Wood v Beves.*

Postal interceptions

121. The Australian Postal Corporation Act 1989 allows for the interception of letters and articles sent by post where the interception is made by the ASIO or where necessary for the enforcement of the criminal law.[181] Where the information relates to the commission of an indictable offence, the Australian Security Intelligence Organisation Act 1979 permits disclosure to State or federal police.[182] It is unclear whether there is any subsequent restriction on use of postal intercepts as evidence in criminal proceedings.

Disclosure of intercept material

122. In addition to the safeguards provided by the legislation authorising the use of intercept evidence, Australian law provides a number of safeguards to prevent the disclosure of sensitive intelligence material contrary to the public interest. First, common law principles governing pre-trial disclosure allow for the same exclusions on public interest immunity grounds as in the UK.[183] Secondly, the Evidence Act 1995 allows the court a broad power to exclude material relating to a 'matter of state' if the public interest in admitting it 'is outweighed by the public interest in preserving secrecy or confidentiality'.[184] Thirdly, the National Security Information (Criminal and Civil Proceedings) Act 2004 provides a special statutory procedure for the non-disclosure of unused sensitive intelligence material in cases involving national security.

123. At the State level, Victoria has similarly enacted the Terrorism (Community Protection Act) 2003 (Vic), which allows the court to exempt disclosure of any information where that disclosure would either 'prejudice the prevention, investigation or prosecution of a terrorist act or suspected terrorist act'; and the 'public interest in preserving secrecy or confidentiality outweighs the public interest in disclosure'.[185]

---

[181] See section 90G and Part 7B generally.

[182] Section 18(3)(a).

[183] See Australia Law Reform Commission Report, 2004.

[184] Section 130(1). Note that several States (e.g. Victoria) do not apply the Evidence Act but instead apply common law principles. As far as the relevant provisions are concerned, however, the common law powers are identical.

[185] Section 23.

Canada

124. Under the Canadian Constitution, criminal law is exclusively a federal matter.[186] Part 6 of the federal Criminal Code is therefore the primary legal framework for the interception of communications by law enforcement agencies in Canada, whether federal, provincial or local.[187] As La Forest J noted in the Canadian Supreme Court decision of *R v Duarte*:[188]

> Electronic surveillance plays an indispensable role in the detection of sophisticated criminal enterprises. Its utility in the investigation of drug related crimes, for example, has been proven time and again. But … it is unacceptable in a free society that the agencies of the state be free to use this technology at their sole discretion. The threat this would pose to privacy is wholly unacceptable. It thus becomes necessary to strike a reasonable balance between the right of individuals to be left alone and the right of the state to intrude on privacy in the furtherance of its responsibilities for law enforcement. Parliament has attempted to do this by enacting Part [6] of the Code. An examination of Part [6] reveals that Parliament has sought to reconcile these competing interests by providing that the police must always seek prior judicial authorization before using electronic surveillance.

125. The Canadian Security Intelligence Service Act 1984 governs interceptions for intelligence purposes carried out by the Canadian Security Intelligence Service ('CSIS').

Law enforcement interceptions

126. Part 6 of the Criminal Code is concerned with the interception of 'oral communications or telecommunications'.[189] The interception of mail is regulated separately.[190] The Code provides that police may apply to a judge for authorisation to intercept communications where there are reasonable grounds to believe the interception may assist the investigation of the offence.[191] The judge must, in turn, be satisfied that it would be in the best interests of the administration of justice to authorise the intercept,[192] and also that either other investigative

---

[186] Section 91(27) of the Constitution Act 1867.

[187] Criminal Code (R.S., 1985, c. C-46)

[188] [1990] 1 SCR 30, at 44-45.

[189] See definition of 'private communication' in section 183.

[190] See primarily the Canada Post Corporation Act (R.S., 1985, c. C-10). Power to intercept mail is also granted under the Customs Act and the Proceeds of Crime (Money Laundering) and Terrorist Financing Act 2000.

[191] Section 185(1)(e).

[192] Section 186(1)(a)

procedures are unlikely to succeed or that, due to urgency, would be impractical.[193] Note that this latter requirement does not apply in the case of interceptions involving terrorist offences or serious organised crime.[194] Police may also intercept communications without a warrant on an emergency basis, 'to prevent an unlawful act that would cause serious harm to any person or to property'.[195]

Admissibility

127. Interceptions authorised under the Criminal Code are admissible as evidence in criminal proceedings.[196] In order to introduce such evidence, however, the prosecution is required to give reasonable notice to the defendant, together with a transcript or written statement containing the particulars of the communication and the time, place and date of the communication and the parties thereto, if known.[197]

Disclosure to the defence

128. Part 6 provides that details of any intercept authorisation are to remain sealed, unless (among other things) ordered by a judge for the purposes of disclosure at trial.[198] Where a defendant[199] applies for an authorisation to be disclosed, section 187(4) provides that the judge shall not allow disclosure until the prosecutor has deleted any part of the document that the prosecutor believes 'would be prejudicial to the public interest'. This includes any material that would:

(a) compromise the identity of any confidential informant;
(b) compromise the nature and extent of ongoing investigations;

---

[193] Section 186(1)(b)

[194] Section 186(2)

[195] Section 184.4(b). Other safeguards against abuse include the reasonable belief of police that warrant could not be obtained despite reasonable diligence (s184.4(a)) and that one of the parties to the communication is the victim or likely victim (s184.4(c)). See also similar provisions for emergency interception without warrant under section 184.1.

[196] The sole exceptions are where the material is legally privileged (section 189(6)) or where the judge is satisfied that the authorisation of an interception granted on an emergency basis is substantially the same as one granted before (section 187(5)). Similarly, evidence from an emergency interception obtained without an authorisation under section 184.1(2) is only admissible in proceedings in which actual, attempted or threatened bodily harm is alleged.

[197] Section 189(5).

[198] Section 187(1.5)

[199] Or any other affected party. Although s187(4) sets down a mandatory disclosure procedure in criminal cases, sections 187(1.3) and (1.4) are drafted in terms that would allow any party to apply for disclosure.

(c) endanger persons engaged in particular intelligence-gathering techniques and thereby prejudice future investigations in which similar techniques would be used; or

(d) prejudice the interests of innocent persons.

129. As Sopinka J noted in *Dersch v Canada (Attorney General)*:[200]

> The purpose of the confidentiality provision of this section is apparently to ensure that the investigation is kept secret during the currency of the authorization and to protect informers, police techniques and procedures once the authorization is spent.

In turn, section 187(7) allows the trial judge, on application by the accused, to make available any deleted material to the defence where he is satisfied that disclosure is necessary 'in order for the accused to make full answer and defence and for which the provision of a judicial summary would not be sufficient'.

Intelligence interceptions

130. Under section 21 of the Canadian Security Intelligence Service Act 1984, the Solicitor General of Canada can authorise the Director of CSIS to apply to a security-cleared judge for a warrant to intercept communications for the purposes of obtaining foreign intelligence or to investigate a threat to the security of Canada.[201] The provisions and safeguards of Part 6 of the Criminal Code do not apply to interceptions authorised under section 21 of the Act.[202] The 1984 Act makes no specific provision for the admissibility or inadmissibility of material intercepted under section 21.

---

[200] [1990] 2 S.C.R. 1505 at 1510, dealing with an earlier version of s187.

[201] Section 21(1).

[202] Section 26.

Hong Kong

Interceptions pre-August 2006

131. Until August 2006, the interception of communications in Hong Kong was regulated by two pieces of legislation: the Telecommunications Ordinance (Cap 106) and the Postal Ordinance (Cap 98). The former required the Chief Executive of Hong Kong to authorise all telecommunication interceptions but gave him wide discretion to do so 'if he considers that the public interest so requires'.[203] Postal intercepts, by contrast, were made under warrant issued by the Chief Secretary for Administration.[204]

132. An Interception of Communications Ordinance was passed in 1997 but never brought into force. In its absence, the District Court of Hong Kong ruled in 2005 that the lack of a sufficiently clear legislative framework to regulate covert surveillance and interceptions violated Article 30 of the Basic Law.[205] Nonetheless, although the recordings of private communications were unlawful, the judge found that it was otherwise fair to admit them as evidence.[206]

133. Note that although intercept material was legally admissible in Hong Kong prior to August 2006, the long-standing policy of the Security Bureau and prosecutors was that it was not adduced in evidence in order to avoid applications from defendants for disclosure of unused, exculpatory material.[207] As part of its recommendations on a new legal framework for covert surveillance, the Law Reform Commission of Hong Kong highlighted a range of arguments in favour of the admissibility of intercept evidence.[208] However, the Hong Kong Security Bureau argued strongly for enacting a statutory prohibition against admitting material from telecommunication intercepts.[209]

---

[203] Section 33 of Telecommunications Ordinance.

[204] Section 13 of the Post Office Ordinance.

[205] *HKSAR v Li Man Tak* [2005] HKEC 1309 at para 55 per Sweeney J. Article 30 of the Basic Law provides that the privacy of communications may not be infringed except to meet the needs of public security or of investigation into criminal offences.

[206] Ibid, para 65.

[207] See HKSAR v Mo Yuk Ping [2005] HKEC 1318 at para 12, per Wright J: 'intercepts are not used for the purposes of gathering evidence for use in criminal proceedings but solely for the purposes of gathering intelligence in regard to criminal activities'. See also Hong Kong Law Reform Commission, *Privacy: the Regulation of Covert Surveillance*, March 2006. PUT CITE and the New York Times (06/08/06) reports that prosecutors seldom introduce evidence in court based on covert surveillance partly to avoid having to answer questions from defence lawyers about the surveillance and about whether any exculpatory evidence was also gathered.

[208] Ibid.

Interceptions post-August 2006

134. In August 2006, the Legislative Council passed the Interception of Communications and Surveillance Ordinance (Cap 589). It created a three-judge panel responsible for authorising and overseeing the use of covert surveillance for security and law enforcement purposes. The Ordinance provides that authorisation of interceptions and other surveillance may be sought on the grounds of preventing or detecting serious crime or the protection of public security.[210] In the case of interceptions, authorisation may only be given by a panel judge. Interceptions may also be authorised in an emergency by a head of department, but must be confirmed by a panel judge as soon as reasonably practicable.

135. The Ordinance covers both interception of telecommunications and post. However, it also distinguishes between the two categories of interception as far as admissibility is concerned. Section 61(1) of the Ordinance provides that telecommunication intercepts are not admissible in legal proceedings, on terms very similar to the current statutory ban in the UK under section 17 RIPA. However, postal interceptions continue to remain admissible under Hong Kong law.[211]

---

[209] See *Proposed Legislative Framework on Interception of Communications and Covert Surveillance* (Security Bureau: February 2006).

[210] Section 3.

[211] See section 59 which provides that postal intercept material be destroyed when retention 'ceases to be necessary for the purposes of any civil or criminal proceedings before any court that are pending or are likely to be instituted', (section 59(3)(a)(iii)) as opposed to telecommunication intercepts, which are to be destroyed 'as soon as reasonably practicable' (section 59(2)(b)).

Ireland

136. The Republic of Ireland is a member of the Council of Europe and party to the European Convention on Human Rights. This was incorporated into Irish law by the European Convention on Human Rights Act 2003. In addition, fundamental rights are given constitutional protection under the 1937 Constitution.[212]

137. The legal framework for the use of covert surveillance by police and other government agencies in Ireland is contained in the Postal and Telecommunication Services Act 1983 and the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993, with the latter introduced to limit the circumstances in which interceptions may be lawfully carried out and introduce safeguards for the protection of personal privacy.

138. Thus, whereas the 1983 Act allows the Minister for Posts and Telegraphs broad scope to issue directions to *An Post and Board Telecom Eireann* to intercept communications,[213] the 1993 Act, by contrast, limits the Minister's power to authorise interception of communications only for the purposes of criminal investigation of the interests of state security.[214] Among the conditions for authorising interception for the purposes of criminal investigation are that other investigations are unlikely to produce 'evidence for the purpose of criminal proceedings'.[215] Authorisations for security purposes do not have this condition.[216] Authorisations are made by the Minister but subject to review by a designated High Court judge and a statutory Complaints referee.[217] As the 1993 Act's title suggests, it applies to both postal and telecommunication intercepts.[218]

139. The admissibility of intercept evidence is governed by section 12(1) of the 1993 Act, which provides that the Minister for Justice is under a duty to make arrangements that 'limit to the minimum necessary the disclosure' of the contents of any intercepted communication, or the fact that it has been made. With the exception of proceedings for unlawful interceptions,[219] however, the Act does not appear to place any specific restrictions on the admissibility of

---

[212] See esp Articles 40-44.

[213] See section 110, allowing the Minister 'to do (or refrain from doing) anything which he may specify from time to time as necessary in the national interest'.

[214] Section 2(1) of the 1993 Act.

[215] Section 4(a)(i).

[216] Section 5.

[217] Sections 8 and 9 respectively.

[218] See the definition of 'communication' in section 1.

[219] Section 10(1) and (2).

intercepted communications as evidence in criminal proceedings. Indeed, the conditions for authorisation under section 4(a)(i) would seem to envisage such use of intercept material.[220]

140. However, although the provisions of the 1993 Act do not prohibit the use of authorised interceptions as evidence *per se*, it appears that the general practice of Gardai and prosecutors is not to rely on intercept evidence at trial. Considerable use is made, however, of telephone records: see for example, the approval of the use of phone records by the Criminal Court of Appeal in the 2005 decision of *DPP* v *Colm-Murphy.* [221]

[220] See also the obiter comments of the Criminal Court of Appeal *in DPP v Colm-Murphy* [2005] IE CCA 1: 'Provided therefore it is established to the satisfaction of the trial court that the interception is being carried out under lawful authority such evidence is in the view of this Court admissible'. The case concerned the admissibility of phone records, however, rather than the contents of intercepts.

[221] [2005] IE CCA 1

New Zealand

Grounds for interception

141. The law governing the lawful interception of communications in New Zealand is spread across a number of statutes, including the Crimes Act 1961, the Telecommunications (Residual Provisions) Act 1986, the New Zealand Security Intelligence Service Act 1969, the Postal Services Act 1998 and the Telecommunications (Interception Capability) Act 2004. Although a number of different Acts allow for the issuing of interception warrants, most follow the same model as that provided by the Crimes Act 1961.[222]

142. Section 216B of the Crimes Act prohibits the use of an interception device to intercept private communications save in certain specified circumstances. Both 'intercept device'[223] and 'private communications'[224] are given an extremely broad definition. The exceptions are primarily relating to those acting with lawful authority, including that conferred by various other statutes for the purposes of national security or investigating serious crime.[225] NZ law does not distinguish between postal and telecommunications intercepts as such: a postal intercept made using an 'intercept device' as defined would therefore fall within the 1961 Act. At the same time, there exist separate specific powers in relation to post.

143. Part 11A of the 1961 Act provides that police may apply to the High Court for a warrant to intercept a private communication using an interception device.[226] In order to do so, the police must have reasonable grounds for believing that (i) a member of an 'organised criminal enterprise'[227] is planning, participating in or committing a specified offence[228] as part

---

[222] The chief exception is warrants issued for the purposes of foreign intelligence under the New Zealand Security Intelligence Service Act 1969.

[223] See section 216A: 'any electronic, mechanical, electromagnetic, optical, or electro-optical instrument, apparatus, equipment, or other device that is used or is capable of being used to intercept a private communication'.

[224] In particular, section 216A does not specify the *medium* but instead refers to 'a communication (whether in oral or written form or otherwise)'.

[225] Section 216B(2)(b).

[226] The definition of 'interception device' under section 312A is subtly different to that under section 216A, and does not refer to 'optical', or 'electro-optical' instruments. Instead, 'interception device' is defined as any 'electronic, mechanical, or electromagnetic instrument, apparatus, equipment, or other device that is used or is capable of being used to intercept a private communication'.

[227] Defined by section 312A as 'a continuing association of 3 or more persons having as its object or as 1 of its objects the acquisition of substantial income or assets by means of a continuing course of criminal conduct'.

[228] See s 247. A 'specified offence' means an offence punishable by 10 years imprisonment or more, conspiring to defeat justice, corrupting juries and witnesses, theft of an object exceeding NZ$1,000 in value, money laundering, or receiving property dishonestly obtained.

of a 'continuing course of criminal conduct';[229] and (ii) it is unlikely that the investigation could be successfully concluded without the issue of the warrant. Applications may also be made where there are reasonable grounds for believing that a serious violent offence[230] or terrorist offence[231] has been, is or is about to be committed and there are reasonable grounds for believing the interception is likely to prevent the commission of the offence. Specific provision for police to apply for interception warrants to investigate drugs offences are provided under the Misuse of Drugs Amendment Act 1978.[232]

144. The New Zealand Security Intelligence Service Act 1969 provides that the Minister in charge of the SIS and the Commissioner of Security Warrants may jointly issue both domestic and foreign interception warrants.[233] Among other things, the interception must be necessary either for the detection of activities prejudicial to the security of New Zealand or for the purpose of gathering foreign intelligence information essential to the security of New Zealand.[234] More generally, Government Communication Security Bureau Act 2003 authorises the Bureau to intercept communications of foreign organisations, companies and persons for the purpose of gaining foreign intelligence.[235] A power to lawfully intercept communications without a warrant is also available to police under the International Terrorism (Emergency Powers) Act 1987 where an 'international terrorist emergency' has been declared by Ministers.[236]

145. Although postal intercepts may be made under several of the above Acts, the Postal Services Act 1998 also provides for the interception of postal items if sent in contravention of various criminal law provisions.[237] Similarly, the Corrections Act 2004 authorises prison governors to read prisoners' mail (except for legally privileged material) in order to prevent threats to others or the commission of criminal offences.

146. Lastly, the Telecommunications (Interception Capability) Act 2004, although not directly concerned with authorising interceptions, does require network operators to ensure

---

[229] Section 312B.

[230] Section 312CA

[231] Section 312CC. Terrorist offence is defined by reference to the provisions of the Terrorism Suppression Act 2002.

[232] Section 14.

[233] Section 4.

[234] Section 4A(3).

[235] See generally Part 3 of the 2003 Act.

[236] Sections 10(3)(a) and (b).

[237] Under section 5, these are the Misuse of Drugs Act 1975, Antiquities Act 1975, Trade in Endangered Species Act 1989, Biosecurity Act 1993, or the Customs and Excise Act 1996.

that their telecommunication networks have interception capabilities.[238] Network operators are also required to provide assistance to law enforcement agencies and intelligence and security agencies where authorised to carry out lawful interception.[239]

Admissibility of intercept material

147. There is no prohibition on the use of lawfully intercepted communications as evidence in criminal proceedings under NZ law. Indeed, most statutes providing for the authorisation of intercepts clearly contemplate that intercept material will be admitted as evidence in legal proceedings.[240] Even those Acts that deal with interception for foreign intelligence purposes[241] do not place any restrictions on the use of lawfully intercepted material in criminal proceedings.

Discovery of unused intercept material

148. The prosecution is required to give reasonable notice to the defence of the intention to use lawfully intercepted communications as evidence in criminal proceedings.[242] The prosecution is also obliged to provide the transcript of the material, together with a statement containing details of the communication (i.e. time, date, place and parties). As in UK law, the prosecution are also under a duty to disclose to the defence the existence of any potentially exculpatory material.[243] Similarly, it is open to the prosecution to seek to withhold disclosure of sensitive material under the common law principles of public interest immunity.[244]

---

[238] Section 7. Interception capability refers to the ability of network operators to gather call associated data and/or the content of the communication (see s 8).

[239] Section 13.

[240] Indeed, section 23B of the Evidence Act 1908 states that where communications are intercepted in accordance with s 216B(3) of the Crimes Act (relating to emergency situations) evidence of the communication, or of its substance, is admissible in evidence.

[241] The New Zealand Security Intelligence Act, Government Communication Security Bureau Act, and Telecommunications (Interception Capability) Act.

[242] Section 312L of the Crimes Acts 1961.

[243] *R v Sampson* (1986) 2 CRNZ 267, 269. Note, however, that the Crown's duty of disclosure is also said to be limited to material which is 'material' to the defence: *R v Quinn* [1993] 3 NZLR 146 at 152. As with Article 6 ECHR, the right to a fair hearing and the right to adequate time and facilities to prepare a defence under the New Zealand Bill of Rights Act 1990 are taken to give rise to a right to pre-trial disclosure: *Simpson v MAF* (1996) 3 HRNZ 342 at 354.

[244] See *Commissioner of Police v. Ombudsman*, [1988] 1 NZLR 385 at 400 per Cooke P: 'there are exceptions [to the rule requiring disclosure to the defence] in special cases where disclosure would prejudice the maintenance of the law and in cases of dispute, a Judge of the Court where the proceedings are pending will be able to determine the issue'.

South Africa

149. South African law on the use of intercept evidence is governed by the Regulation of Interception and Provision of Communication-Related Information Act 2002 ('RICA').[245] This replaced the earlier Interception and Monitoring Prohibition Act 1992,[246] following prolonged consultation by the South African Law Reform Commission.[247] The 2002 Act covers both 'direct' and 'indirect' communications.[248] The former is defined as any oral statement made in the immediate presence of another person.[249] The latter covers the 'transfer of information' in the form of speech, music, data, text, visual images, signals, or radio or in any other form transmitted by post or via a telecommunications system.

Applications for interception

150. Section 16 allows law enforcement bodies to apply to a designated judge for an interception direction. The grounds for issuing an interception direction include that a serious offence has been or is being or will probably be committed;[250] and the gathering of information concerning an actual or potential threat to public health, safety, national security or compelling national economic interests.[251] In other words, section 16 includes interception for both law enforcement and intelligence purposes. The designated judge must also be satisfied that other investigative means have either been exhausted, are impracticable, or are too dangerous.[252] This latter requirement does not apply, however, in cases involving serious organised crime.[253] In exceptional cases, police may also intercept communications without prior authorisation in order to prevent imminent serious bodily harm.[254]

151. Notably, the 2002 Act provides that the judge issuing an interception direction may require the law enforcement body applying for the direction to supply written progress reports on the investigation.[255] The judge may thereby cancel the interception direction if satisfied that

---

[245] No. 70 of 2002

[246] No. 127 of 1992

[247] *Report on the Interception and Monitoring Prohibition Act (Act No. 127 of 1992)* (October 1999)

[248] See section 1.

[249] This includes statements made into telephones, etc, but physically overhead by another.

[250] Section 16(5)(a)(i)

[251] Sections 16(5)(a)(ii) and (iii)

[252] Section 16(5)(c)

[253] Section 16(5)(c)(i).

[254] Section 7.

[255] Section 24.

either the objectives have been achieved, the grounds made out for the interception no longer exist, or if the law enforcement body fails to provide written updates as directed.[256]

Admissibility of interceptions

152. Section 47(1) provides that the contents of any communication lawfully intercepted under the 2002 Act are admissible in criminal proceedings.[257] They are also admissibile in certain civil proceedings under the Prevention of Organised Crime Act 1998 (e.g. property forfeiture and criminal assets recovery actions).[258] However, the contents of *any* intercept (whether made in South Africa or elsewhere) may only be used as evidence with the written authority of the National Director of Public Prosecutions.[259]

153. Because interception directions are required to contain a number of details concerning the investigation for which the interception is sought,[260] Chapter 9 also prevents detailed inquiry into the contents of directions in any legal proceedings. Specifically, section 48 of the Act directs that a certificate of a designated judge shall be *prima facie* proof of a valid interception direction for the purposes of any criminal or civil proceedings.

Non-disclosure of unused material

154. As in other common law jurisdictions, the prosecution may seek to withhold disclosure of unused material on the basis of principles of public interest immunity. In *Shabalala v Attorney General of Transvaal*,[261] the Constitutional Court ruled that the prosecution was under a duty to disclose any unused material contained in the police docket (i.e. witness statements, expert reports, internal reports and memoranda, and the diary of the investigation) that were necessary in order for the accused to exercise his right to a fair trial. However, the Court ruled that:[262]

---

[256] See section 25(1).

[257] Section 47(1). The only exception to this under the 2002 Act is where a law enforcement body applies for an interception direction orally but fails to follow it up with a written application within 48 hours. In such circumstances, section 25(5) directs that the contents of any communication will be inadmissible as evidence in any criminal or civil proceeding 'unless the court is of the opinion that the admission of such evidence would not render the trial unfair or otherwise be detrimental to the administration of justice'.

[258] Section 47(1).

[259] Section 47(2).

[260] See e.g. section 16(6)

[261] 1996 (1) SA 725 (CC).

[262] 1996 (1) SA 725 (CC) at 72.

> The State is entitled to resist a claim by the accused for access to any particular document in the police docket on the grounds that such access is not justified for the purposes of enabling the accused to properly exercise his or her right to a fair trial or on the ground that it has reason to believe there is a reasonable risk that access to the relevant document would lead to the disclosure of the identity of an informer or State secrets or on the grounds that there was a reasonable risk that such disclosure might lead to the intimidation of witnesses or otherwise prejudice the proper ends of justice.

155. In August 2002, the South African Law Reform Commission recommended a statutory code for prosecution disclosure.[263] Among the draft provisions, it suggested that prosecution could automatically withhold any material intercepted pursuant to a direction or anything that indicated 'that such a direction has been issued or that material has been intercepted in obedience to such a direction'.[264]

---

[263] *Project 73: Fifth Interim Report on the Simplification of Criminal Procedure* (August 2002),

[264] Clause 104B(7)(b).

United States

156. The primary law governing the interception of communications by law enforcement and intelligence bodies in the United States is federal: Title III of the Omnibus Crime Control and Safe Streets Act 1968[265] ('Title III') and the Foreign Intelligence Surveillance Act 1978 ('FISA'), authorising law enforcement and intelligence interceptions respectively.[266] These provisions were broadened considerably by the passage of the USA PATRIOT ACT 2001[267] ('PATRIOT Act') following the 9/11 attacks. In particular, the PATRIOT Act lifted a long-standing ban on the evidential use of intelligence intercepts under FISA. Postal intercepts, by contrast, are effected using normal search warrants.[268]

Law enforcement interceptions

157. The federal law governing the interception of wire and electronic communications and oral communications for law enforcement purposes is set out in Title III. A 'wire communication' refers to any 'aural transfer' made via wire, cable or 'other like connection' operated for the transmission of 'interstate or foreign communication'.[269] 'Electronic communication' is given a similarly broad definition.[270]

158. Under Title III, the Department of Justice may authorise the FBI to apply to a federal judge for an interception in relation to the investigation of an extremely broad range of federal offences, including most terrorism offences.[271] Similarly, state prosecuting authorities may authorise state law enforcement to apply to a state court judge in relation to a similarly broad range of state offences.[272] The grounds on which a judge shall grant an order authorising interception are:[273]

---

[265] US Code, Title 18, Chapter 119.

[266] US Code, Title 50, Chapter 36.

[267] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. 107-56, 115 Stat. 272 (2001).

[268] The Fourth Amendment protects against interception of first-class mail and parcels without a search warrant. See e.g. *Ex parte Jackson* (1878) 93 US 727, 723.

[269] 'or communications affecting interstate or foreign commerce' (i.e. any public telecommunications network): § 2510(1)

[270] § 2510(12): 'any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce'. It excludes, however, tone pagers, tracking devices and electronic fund transfer information.

[271] § 2515(1)

[272] § 2515(2)

[273] § 2518(3)

- there is probable cause for belief that an individual is committing, has committed, or is about to commit a specified offence;

- normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; and

- there is probable cause for belief that the facilities or place where the communications are to be intercepted are being used in connection with the offence.

159. In practice, the burden of showing that normal investigative procedures have not been or are not likely to be successful has not been difficult for the government to discharge.[274] Interception authorisations last for 30 days, but are renewable.[275] In cases of emergency, interceptions can be made without prior authorisation for a period up to 48 hours.[276] Evidence from any interception made contrary to Title III, including an emergency intercept where authorisation was not sought within 48 hours,[277] is inadmissible in any legal proceeding, state or federal.[278] Note that any application made or order granted under Title III is sealed. No disclosure is permitted save as ordered by another judge of competent jurisdiction.[279]

160. Evidence obtained from an interception under Title III is admissible in criminal proceedings so long as each party receives a copy of the interception application and order within 10 days before the trial.[280] The judge may waive the ten day period, however, where the judge finds that it was not possible to serve the information and that the party will not be prejudiced as a result.[281]

161. Title III also provides a right of any party to seek to suppress the introduction of intercept evidence on the grounds that it was unlawfully obtained, the authorising order was legally deficient, or that the actual intercept failed to comply with the authorising order. The judge may 'in his discretion make available to the aggrieved person or his counsel for

---

[274] See e.g. *United States v Lopez,* 300 F.3d 46, 52 (1st Circuit, 2002): 'the necessity requirement [under §2518] is not tantamount to an exhaustion requirement'.

[275] § 2518(5)

[276] § 2518(7).

[277] § 2518(7)

[278] § 2515

[279] § 2518(8)(b)

[280] § 2518(9)

[281] § 2518(9)

inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice'.[282]

Intelligence interceptions

162. Unlike interception for law enforcement purposes under Title III, 'electronic surveillance' under FISA[283] may be directed at a broad range of targets, including 'foreign powers'[284] and 'agents of foreign powers'.[285] The former includes groups 'engaged in international terrorism or activities in preparation therefor'.[286] The latter includes a US national 'knowingly' engaged in international terrorism 'or activities that are in preparation therefor'.[287]

163. In order to obtain an interception warrant under FISA, a federal officer must apply to a judge certifying – among other things – that a 'significant purpose' of the interception is to obtain 'foreign intelligence information'[288] and that such information 'cannot reasonably be obtained by normal investigative techniques'.[289] The language of 'significant purpose' was an amendment introduced by the PATRIOT Act in order to allow greater use of FISA intercepts for law enforcement purposes.[290]

164. A judge may grant a FISA warrant where he is satisfied, among other things, that there is probable cause that the target of the interception or surveillance 'is a foreign power or an agent of a foreign power'.[291] Interestingly, FISA contains the safeguard that no US citizen may be considered as falling within these categories 'solely on the basis of activities protected by the first amendment to the Constitution of the United States'.[292]

---

[282] § 2118(10)(a)

[283] See § 1801(f)

[284] § 1801(a)

[285] § 1801(b)

[286] § 1801(a)(4)

[287] § 1801(b)(2)(C)

[288] As defined in § 1801(e)

[289] §§ 1804(7)(A), (B) and (C).

[290] Previously, the government had been obliged to certify that obtaining foreign intelligence information was the 'primary purpose' of a FISA intercept. This rule had been established to prevent law enforcement using FISA to evade the more stringent requirements of Title III. In addition, the Justice Department had imposed restrictions on the dissemination of intercept material gained under FISA to prevent its use by law enforcement in criminal investigations. See *In re Sealed Case*, 310 F.3d 717, 727-28.

[291] § 1805(a)(3)

[292] § 1805(a)(3)(A)

165. Following the PATRIOT Act, evidence obtained under a FISA warrant is admissible in legal proceedings. As with material obtained from law enforcement intercepts under Title III, the government or state prosecutor is obliged to give the defendant reasonable notice of the government's intention to rely on intercept evidence obtained under a FISA intercept.[293] Similarly, a defendant may seek a motion to suppress FISA intercept evidence on the basis that it was unlawfully obtained or the surveillance was not made in conformity with the order.[294] In determining any objection to intercept material, the Attorney General may request an *ex parte* hearing of the issue on the basis that 'disclosure or an adversary hearing would harm the national security of the United States'.[295] FISA also permits the court to disclose to the defendant:[296]

> under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

Disclosure of unused material

166. In addition to the procedures laid down under Title III and FISA in relation to challenges to the legality of interceptions, the federal Classified Information Procedures Act 1980 ('CIPA') provides a procedural framework for disclosure of classified information in criminal proceedings.

167. Section 3 of the Act provides that the government may apply for a court order to 'protect against the disclosure of any classified information disclosed by the United States to any defendant in any criminal case'. Section 4 provides the specific means whereby classified information shall be protected, including the deletion of specific items from documents by the prosecution; to provide summaries in place of actual documents; or substituting 'a statement admitting relevant facts that the classified information would tend to prove'. Where the court orders the government to disclose classified material to the defence, the government may instead seek to substitute a summary of the information or a statement admitting relevant facts.[297] The court is obliged to grant the government's motion 'if it finds that the statement or summary will provide the defendant with substantially the same ability to make his defence as would disclosure of the specific classified information'.

---

[293] §§ 1806(c) and (d)

[294] § 1806(e)

[295] § 1806(f)

[296] § 1806(f)

[297] Section 6(c).

Conclusions

168. Having examined the arguments for and against the use of intercept evidence in Part 2, we are left with the conclusion that the UK government's ban is archaic, unnecessary and counter-productive. For too long, it has been taken as axiomatic that using intercept material in courts would lay bare methods of interception and allow criminals and terrorists to evade detection in their activities. At the same time, UK courts have developed common law principles of public interest immunity ('PII') to protect a wide range of sensitive information from being unnecessarily disclosed in criminal proceedings.

169. While UK authorities have been unwilling to allow PII principles to protect interception capabilities in the UK, the survey of common law jurisdictions in Part 3 shows that PII-principles have been used by the great majority of common law countries – Australia, Canada, New Zealand, South Africa and the United States – in order to facilitate the use of intercept evidence in adversarial criminal proceedings. Nor have the UK government been able to point to any evidence to show that the regular use of intercept evidence in these countries has led to a degradation of interception capabilities.

170. We therefore recommend that the ban on intercept evidence in UK courts be lifted. Rather than simply amend section 17 RIPA to allow its use, however, we recommend that the legal framework governing the authorisation of lawful interception of communications by law enforcement and intelligence services should be redrawn. In particular we recommend the power of the Home Secretary to issue interception warrants for both intelligence and law enforcement purposes should be replaced with a scheme for judicial authorisation of interceptions. This would bring the UK into line with the practice of virtually every other common law country.[298]

171. For the reasons given in Part 2, we consider that the existing procedures for PII applications under the Criminal Procedure and Investigations Act 1996 are sufficient to prevent sensitive information, including information about interception capabilities, being disclosed contrary to the public interest.

172. However, based on the experience of other common law jurisdictions, we would support the adoption of a provision along the lines of that contained in section 48 of the South African Regulation of Interception and Provision of Communication-Related Information Act 2002, whereby a certificate by a judge authorising an interception shall be taken as *prima facie* proof of a valid interception authorisation for the purposes of any subsequent criminal or civil proceedings. Alternatively, the practice of sealed interception authorisations as set out in

[298] See our 1998 Report, Recommendation 2, pp 19-22.

Part 6 of the Canadian Criminal Code, accompanied by a structured judicial procedure for disclosure to defendants seems to us an acceptable way of balancing the public interest in maintaining a covert interception capability and the defendant's right to a fair trial.[299]

173. Lastly, we leave open the question of whether there should be separate warrants for intelligence and law enforcement purposes, as is currently the case in a number of jurisdictions, or a single warrant applicable to either purpose. We are aware that one proposal under consideration in government studies is the 'triple warrant model',[300] comprising (i) intelligence warrants, (ii) 'non-evidence' warrants for law enforcement purposes and (iii) evidence warrants. As the names suggest, only material obtained pursuant to an evidence warrant would be admissible in legal proceedings. Originally, all warrants issued would be either intelligence or non-evidence warrants but a non-evidence warrant could subsequently be converted to an evidence warrant following judicial authorisation.

174. However, although we recognise that the duties to retain, record and disclose intercept material can be problematic,[301] the triple-warrant model seems to us to lack parsimony. In particular, given that one of the difficulties with Part I of RIPA is its undue complexity, we question the wisdom of replacing one overly-complex legislative scheme with another. We mean to address the issue if and when detailed proposals are brought forward. For the present time, it suffices to note that the trend in other common law countries is towards a single warrant model whose product is admissible regardless of the original purpose, whether by making intelligence warrants admissible in criminal proceedings (such as provided in the US by the PATRIOT Act) or by the establishment of a single warrant structure, such as under the 2002 South African legislation. Again, we see no objection in principle to the admissibility of intelligence interceptions as evidence so long as the interception itself is lawful and compatible with fundamental rights. Nor are there any circumstances in which the intelligence services would be forced to disclose material that they fear would compromise national security – should such disclosure ever be required in a particular case, it is always open to the prosecution to withdraw the charges.

175. Nothing we recommend here, however, should be taken as any kind of support for broadening the available grounds for lawful interception in UK law, still less any kind of evidence gathering by way of unlawful interception. As we recommended in our 1998 report on covert policing, any interception of private communications should be attended by careful

---

[299] See section 187(4) above.

[300] Kingsley Hyland paper

[301] As the Hong Kong Law Reform Commission noted in its 2006 report, n22 above, the issue of retention of intercept material for subsequent criminal proceedings is highly problematic.

safeguards. In particular, interceptions must only be authorised where necessary and proportionate having regard to fundamental rights.

176. Indeed, it may seem strange to some that a human rights organisation should argue for the evidential use of intercept material in criminal cases. As explained at the outset, however, the UK prohibition on the use of intercept evidence is maintained at a time when evidential difficulties in terrorism cases have been used to justify surprising and significant departures from fundamental rights and the rule of law. As the President of the Supreme Court of Israel, Aharon Barak, said in 2002:[302]

> While terrorism poses difficult questions for every country, it poses especially challenging questions for democratic countries, because not every effective means is a legal means. I discussed this in one case, in which our Court held that violent interrogation of a suspected terrorist is not lawful, even if doing so may save human life by preventing impending terrorist acts.
>
> This is the fate of democracy, as not all means are acceptable to it, and not all methods employed by its enemies are open to it. Sometimes, a democracy must fight with one hand tied behind its back. Nonetheless, it has the upper hand. Preserving the rule of law and recognition of individual liberties constitute an important component of its understanding of security.

The self-evident corollary of Barak's statement is surely that democracies should not deny themselves the legitimate and effective means that *are* available to them, of which the evidence gained from lawful interceptions of communications is surely one. Intercept evidence may not be a silver bullet but it is a bullet nonetheless. The time has come for the UK to join the ranks of common law countries that allow such ammunition in the fight against terrorism.

---

302 'A Judge on Judging: The Role of A Supreme Court in A Democracy', *Harvard Law Review*, Vol. 116, No. 1 (November 2002), pp 19-162 at 148.

Appendix A: support for intercept evidence

Police

Sir Ian Blair, Metropolitan Police Commissioner, February 2005:[303]

> I have long been in favour of intercept evidence being used in court. The court can then weigh it up. At the moment nobody can test it.

Andy Hayman, Assistant Metropolitan Police Commissioner and Chair of the National Counter Terrorism Tasking and Coordinating Group:[304]

> I originally started off by being fairly unsupportive of the notion of using [intercept evidence], mainly on the basis that it was starting to disclose methodology to the other side …. I think I am moving … to a conclusion that in a selected number of cases, not just for terrorism but also for serious crime, it would be useful. I think also it does make us look a little bit foolish that everywhere else in the world is using it to good effect.

Prosecutors

Ken Macdonald QC, Director of Public Prosecutions:[305]

> The sooner we can use intercept evidence, the sooner we can stop talking about secret courts and detention without charge. When it comes to protecting sources and techniques from probing questions from the defence, we already have public interest immunity hearings, which determine whether a full transcript would assist the defence, or undermine national security… the fear that the way it is all done will be revealed to a lucky defendant is wrong. And you can always walk away from the case.

Sir David Calvert-Smith QC, former Director of Public Prosecutions:[306]

> [Allowing intercept evidence] would assist us enormously. As prosecutors, our lives would be made much easier. I'm quite sure there are cases where important evidence, which would have strengthened the prosecution, is having to go by the board.

---

[303] 'Lift phone tap ban in terror trials, says new Met chief' by Rachel Sylvester, Daily Telegraph, 5 February 2005.

[304] Evidence to House of Commons Home Affairs Committee, 28 February 2006, Q224.

[305] Law Society Gazette, 'Human rights lawyers back Goldsmith call to use intercept evidence in court', 28 September 2006.

[306] The Observer, 'Juries should hear phone taps to nail crime gangs', by David Rose, 8 September 2002.

Parliamentary Committees

Joint Committee on Human Rights:[307]

> In our view, the ban on the use of intercept evidence in court should now be removed, and attention should be turned urgently to ways of relaxing the ban.

House of Commons Home Affairs Committee:[308]

> Outside the Government there is universal support for the use of intercept evidence in the courts. The Home Office has not produced convincing evidence that the difficulties are insuperable: they have presumably been tackled in other jurisdictions. We therefore urge the Government to conclude its review of the issue, with the aim of reporting as soon as possible. In the absence of any new information, we assume that it will recommend the use of intercept evidence.

Professional Bodies

Guy Mansfield QC, Chair of the Bar Council of England and Wales:[309]

> The current law is illogical. Broadly speaking, telephone intercept evidence cannot be used. However, telephone intercepts lawfully obtained in foreign jurisdictions are admissible in English courts. A tape recording of a telephone conversation made by one of the participants is admissible. Conversations recorded from a bug legally planted in premises used by drug dealers are admissible, and such conversations can include what is said by a suspect into the telephone. There is no logical reason why intercept evidence should not be admissible primary evidence. It is contemporaneous evidence. It can be persuasive and compelling. It is admissible under the common law, and has only been banned by Parliament. The use and extent of intercept evidence should be decided on a case-by-case basis.

Law Society of England and Wales:[310]

> The decision to maintain the ban on the use of communication intercept evidence is puzzling as well as disappointing. The Society believes the inclusion of intercept evidence would be a

---

[307] *Counter-Terrorism Policy and Human Rights: Prosecution and Pre-Charge Detention* (HL 240/HC 1576: July 2006), para 101.

[308] *Terrorism Detention Powers* (HC 910: June 2006), para 116.

[309] Bar Council, 'Intercept evidence – no legal or operational problem with using it in court', 18 February 2005.

[310] Law Society briefing for Second Reading of the Prevention of Terrorism Bill, 2 March 2005.

positive step forward in enabling the effective prosecution of terrorist suspects. The government has not adequately explained why this cannot work in the UK when it is commonplace in other jurisdictions.

Independent reviews

Lord Lloyd of Berwick, author of the 1996 review of counter-terrorism legislation:[311]

> We have here a valuable source of evidence to convict criminals. It is especially valuable for convicting terrorist offenders because in cases involving terrorist crime it is very difficult to get any other evidence which can be adduced in court, for reasons with which we are all familiar. We know who the terrorists are, but we exclude the only evidence which has any chance of getting them convicted; and we are the only country in the world to do so.

Newton Committee of Privy Counsellors:[312]

> [O]ne way of making it possible to prosecute in more cases would be to remove the UK's self-imposed blanket ban on the use of intercepted communications in court …
>
> … We recognise that a balance has to be struck between the public interest in prosecuting particular cases and the public interest in maintaining the effectiveness of intelligence gathering techniques and capabilities. We consider, however, that the balance has not been struck in the right place if intercepted communications can never be used evidentially.

Lord Carlile of Berriew QC, independent statutory reviewer of terrorism legislation:[313]

> [T]he potential to use intercept evidence should be available. This would not mean that it would have to be used. In a small number of terrorism cases, and probably a larger number of drug-smuggling and money-laundering cases, and possibly in other categories of crime especially with an international dimension, it would help to secure convictions.

---

[311] See Hansard, HL Debates, 19 June 2000, Col. 109-110.

[312] *Report of the Privy Counsellors Review of the Anti-Terrorism Crime and Security Act 2001* (HC 100: 18 December 2003), paras 208, 212/

[313] Lord Carlile of Berriew QC, *Proposals By Her Majesty's Government For Changes To The Laws Against Terrorism,* 6 October 2005.

Politicians

Lord Goldsmith QC, Attorney-General of England and Wales:[314]

> I'm personally convinced we have to find a way of avoiding the difficulties [of using intercept evidence]. I do believe there are ways we can do that. Otherwise, we're depriving ourselves of a key tool to prosecute serious and organised crime and terrorism.

David Davis MP, Shadow Home Secretary:[315]

> We are virtually the only major country in the world that does not use intercept evidence in court. That must make it even more difficult to bring terrorist cases to trial, and as such, degrades both our safety and our system of justice.

Sir Menzies Campbell MP, leader of the Liberal Democrats:[316]

> We must never give in to terrorists. They should be pursued through international co-operation and stronger intelligence services. But, we do not need impractical policies like ID cards, but rather the use of intercept evidence, as in every other Western nation.

---

[314] The Guardian, 'Courts set to admit wiretap evidence', by Clare Dyer, 21 September 2006.

[315] Hansard, HC Debates, 26 January 2005 : Column 310.

[316] 8 June 2006.

Table 1: Comparative use of intercept evidence in common law jurisdictions

Jurisdiction	Criminal process	Authorisation for interception	Telecom intercepts	Postal intercepts	Disclosure
Australia	Adversarial	Judge*	Admissible	Admissible	Evidence Act 1995 and NSIA 2004
Canada	Adversarial	Judge	Admissible	Admissible	Part VI, Criminal Code 1985
Hong Kong	Adversarial	Judge	Inadmissible	Admissible	ICSO 2006
Ireland	Adversarial	Minister for Justice	Admissible**	Admissible**	IPPTMA 1993
New Zealand	Adversarial	Judge	Admissible	Admissible	Common law
South Africa	Adversarial	Judge	Admissible	Admissible	Common law
United States	Adversarial	Judge	Admissible	Admissible	CIPA 1980
United Kingdom	Adversarial	Home Secretary	Inadmissible	Inadmissible	CPIA 1996

* For law enforcement interceptions only. The Attorney General issues national security warrants for interceptions

**Although technically admissible, the Irish authorities do not rely on intercept evidence in criminal prosecutions.

NSIA = National Security Information (Criminal and Civil Proceedings) Act 2004

ICSO = Interception of Communications and Surveillance Ordinance 2006

IPPTMA = Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993

CPIA = Classified Information Procedures Act 1980