PRIVY COUNCIL REVIEW OF INTERCEPT AS EVIDENCE

REPORT

to the Prime Minister and the Home Secretary

30 January 2008

Cm 7324

PRIVY COUNCIL REVIEW OF INTERCEPT AS EVIDENCE

REPORT

to the Prime Minister and the Home Secretary

30 January 2008

Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty

February 2008

CM 7324

£9.25

We wish to express our warm appreciation and gratitude to the staff of this Review. The Secretary, Owen Rowland, and David Garland have brought unfailing lucidity, resourcefulness, judgment and skill to our work, and we are particularly appreciative of the efficient and constant support which Jane Galloway gave to us and them.

We owe thanks more widely than we can sensibly list here to all those who have helped us across many departments and agencies, and other organisations and individuals outside Government. We owe a particular debt of gratitude to Linda Bickerton and to Angela Mark and her team who, though not members of our staff, were always most helpful and considerate. Without their support, our work would not have been possible and we thank all of them.

Rt Hon Sir John Chilcot GCB
Rt Hon Lord Archer of Sandwell
Rt Hon Alan Beith MP
Rt Hon Lord Hurd of Westwell

PRIVY COUNCIL REVIEW OF INTERCEPT AS EVIDENCE

CHAPTER I – INTRODUCTION

1. On 25 July 2007, the Prime Minister announced that he and the Home Secretary had established a Privy Council Review with the following Terms of Reference:

'To advise on whether a regime to allow the use of intercepted material in court can be devised that facilitates bringing cases to trial while meeting the overriding imperative to safeguard national security.

It will consider:

- *The benefits that might reasonably be expected to result from such use (in terms, for example, of increases in the number of successful prosecutions in serious organised crime and terrorism cases);*
- *The risks, including from exposure of interception capabilities and techniques;*
- *The resource implications of any changes in the law;*
- *The implications of new communications technology; and*
- *The experiences of other countries and their relevance to the UK.'*

2. This Report is the outcome of that Review. We describe how interception is currently authorised and used in the UK, and estimate the benefits interception currently brings through its use as intelligence as well as the potential further benefits it could bring if used as evidence. We examine the risks and resource implications of using intercept as evidence, and the changes that are likely to result from new communications technology now coming into widespread use. We cover in some detail the experiences of other countries (almost all of which use intercept as evidence), and what they teach us. We examine the many different legal models that have been proposed for evidential use of intercept in the UK. Finally, we set out our conclusions from all of this and list our recommendations.

3. The question posed to the Review may at first sight seem simple, especially given the widespread use of intercept as evidence across the world. It is in fact far from straightforward. All the bodies and individuals that met with or provided written views to this Review were in favour in principle of intercept as evidence. **We are in agreement with this.** But once that principle was stated, there were very different views on whether national security could be safeguarded effectively, and whether the benefits of intercept as evidence outweighed the risks and costs.

4. These different views were in almost all cases strongly held, and in many instances have been the firm views of the organisations involved for many years. However, some of those involved have changed their views in the light of experience. The arguments they bring, for and against intercept as evidence, are by their nature asymmetric. Those in favour of intercept as evidence make their case on the basis of openly available material. Those who believe that the case has not been made, or that a model with the necessary safeguards has not been found, cannot put their case fully in

public, as at least key parts of it rely on classified material, for example the nature, scale and benefit of the current use of intercept as an intelligence and investigative tool, and the risks to which it is exposed. For reasons of national security and to preserve confidences, the public version of our Report unavoidably omits some of the most telling details of the case against evidential use, which are nonetheless very important in reaching a judgement. Such redactions are indicated by the symbol ***. ***

5. The arguments also differ in character. Those in favour of allowing the use of intercept as evidence make a combination of arguments of principle and practical benefits. They assert the importance of combating terrorism and serious organised crime through prosecuting those responsible and making the best evidence available to courts. They also believe that evidential use of intercept would result in more successful prosecutions of serious organised criminals and terrorists, and reduce the need for other measures to protect the public which have proven unpalatable or at least controversial. Those who are against evidential use, while accepting the principle of using the best available evidence to prosecute when possible, argue that the current use of intercept as intelligence brings many of the practical benefits of using intercept material directly. They also refer to risks and operational impact, including the resource impact, of any change on national security including prevention, disruption and prosecution of serious crime and terrorism. We have had continually to balance both sets of arguments.

6. The principles which almost all witnesses are agreed on, and which this Review endorses, include:

- There is an overriding imperative to safeguard national security. It is a basic function of the State to protect the public from threats such as international terrorism. Chapter II describes the critical contribution which interception makes to intelligence, and Chapter IV notes some of the risks to that contribution posed by evidential use of intercept. Legal models, referred to in Chapter VIII, have the general aim of building safeguards in order to eliminate these risks or reduce them to an acceptably low level.
- All trials must be (and be seen to be) procedurally fair. That requirement is encapsulated in Article 6 of the European Convention on Human Rights (ECHR), but has of course been part of English Common Law since its origin. The concept of a fair trial can accommodate national security considerations to some extent, provided there are sufficient safeguards to mitigate any potential unfairness to the defendant. But ultimately the ability to ensure a fair trial in any particular case and the need to safeguard national security may not be reconcilable. In that case the only remaining option for the State will be not to prosecute or if proceedings have already commenced, to pull the case.
- The State should wherever possible prosecute those it believes are involved in terrorism or other serious crimes.
- In any criminal prosecution the best available evidence (for and against the accused) should be made available to the court. This will best achieve the aim of convicting the guilty, while minimising the risk of

miscarriages of justice. A class of potential evidence (such as intercepted material) should only be excluded if there are powerful reasons for doing so.

7. The challenge of this Review has therefore been to judge, on the basis of the best available evidence, whether a legal and operational regime could be devised which allows for the evidential use of intercept in line with these principles. The Terms of Reference set out a clear set of issues to consider, which provide the basis of the structure of the Report. Nevertheless our task has not been simple. The benefits and risks of intercept as evidence involve a complex interplay of legal, operational, technical, resource and organisational matters of principle and practice. The issue is one of critical judgement, rather than absolute assertion, and this has been acknowledged by most witnesses.

8. It is also an issue of confidence: if key contributors to intelligence-gathering do not believe that the security of the process is completely protected, sources of intelligence may dry up, or their concerns may in practice preclude the use of any new power to deploy intercept as evidence. On the other hand there can be a lack of confidence in a criminal justice system where evidence which might be crucial in reaching a just verdict is withheld by law.

9. We have had to consider from a broad perspective whether a regime for intercept as evidence can be developed that safeguards national security, (including our ability to prevent and disrupt serious crime and terrorism - which often requires operational speed and flexibility), and at the same time will allow more successful and fair prosecutions. We have attempted to assess and weigh the potential benefits of intercept as evidence, based upon a workable legal regime, against the risks and costs, including any impact on the current use of intercept.

10. In this exercise we believe, as foreshadowed in our terms of reference and set out more fully in Chapter II, that the UK's strategic intelligence capability must not be compromised. By contrast, the current use of interception as intelligence to serve tactical operational requirements (such as the disruption of terrorist and serious crime networks) and to support law enforcement through prosecutions based on evidence often derived from intercept, but not based on using it evidentially; and its potential future use directly as evidence are both (by no means mutually exclusive) ways of supporting the same objectives of combating terrorism and serious crime. We have attempted to judge the value of their respective contributions to the prevention, disruption and prosecution of terrorists and serious criminals, and how the introduction of intercept as evidence would be likely to affect these contributions.

11. This is the seventh report to Ministers on the issue of intercept as evidence in the last thirteen years, but it is the first to have been produced by people who are not currently within government. It is based upon the latest material available, including meetings with nearly 40 individuals and over 30

written submissions received. It also builds upon the extensive work conducted by the previous reviews, and in particular on the large corpus of legal advice obtained by those reviews. In addition, we have also obtained independent legal advice on those models we considered still to be viable, as set out in Chapter VIII. A number of bodies outside Government have also recently produced reports on this issue, which have been of considerable interest and help to this Review.[1]

12. We recognise the serious, creative efforts made over the years, to find a solution, so far without success. It has not been a case of rigid, unthinking resistance to change. However, as the issue has been debated at great length over so many years, most of those engaged in the debate have arrived at firm, but opposing, conclusions already. Our approach has been to re-open the arguments, where possible with participants from both standpoints, and review from scratch both the assertions, and the analyses, made on both sides.

13. Since one of the most telling arguments in favour of change is the positive experience of so many other countries, we have devoted much time to reviewing what actually happens in a selection of other countries. We have visited, received submissions from or met individuals from twelve different countries. We have considered carefully the degree to which their experiences can inform the UK approach.

14. The telecommunications industry is evolving very rapidly, and interception has to react to that. We have therefore also considered at some length the particularly complex implications of the new technology, and its potential impact on the benefits, costs and risks of any intercept as evidence regime.

[1] See Bibliography at Annex D

CHAPTER II - CURRENT USE OF INTERCEPT

INTERCEPTION IN THE UK

15. Interception of communications in the UK is governed by the Regulation of Investigatory Powers Act 2000 (RIPA), which provides various grounds on which interception will have "lawful authority", including when conducted under warrant. The term 'interception' covers a wide variety of related techniques, which can give legally authorised access to communications ranging in sophistication from an ordinary call between two fixed telephones in the UK to a complex multi-media session *** running across broadband connections *** (for more detail see Chapter VI). In the future even more sophisticated media will come onto the market, and interception will have to provide access to as many of them as its targets choose to use. Interception covers the post as well as electronic media.

16. Interception in accordance with the UK's legal framework under RIPA provides both tactical and strategic information for the intelligence and law enforcement agencies. Tactical interception provides real time intelligence on the plans and actions of individual terrorists, criminals and other targets, which allows the agencies to disrupt their plans and frustrate their actions. It can identify evidence against the targets and facilitate their arrest. Strategic interception can reveal the existence of new targets, as well as the significance, long term plans, international connections and modus operandi of existing targets, from which (with intelligence from other sources) a broad understanding of the terrorist and criminal threat facing the UK can be derived and preventive strategies developed.

THE CURRENT LAW

17. RIPA permits specified intelligence and law enforcement agencies to intercept all forms of communications (by post as well as electronically) on the authority of a warrant given by the Secretary of State. A warrant can be given for any of three purposes

- In the interests of national security
- For the purpose of preventing or detecting serious crime
- For the purpose of safeguarding the economic well-being of the United Kingdom.

In Scotland, warrants for the purpose of preventing and detecting serious crime are given by Ministers in the Scottish Executive.

18. Before giving a warrant, the Secretary of State or Scottish Minister must be satisfied that interception is necessary to obtain the information required; that the information could not reasonably be obtained by other means; and the interception is proportionate to what it seeks to achieve. Warrants last for three or six months depending on purpose, but can be renewed by the Secretary of State or Scottish Minister. Warrants covering interception of communications or post within the UK can cover only one person or premises; different telephone numbers etc. used by the same target

are included in a schedule, which can be modified quickly if, for example, the target begins to use a new mobile phone.

19. The activities and decisions of the Secretary of State, the Scottish Ministers and the intercepting agencies are overseen by the Interception of Communications Commissioner, a senior judge appointed for the purpose by the Prime Minister. The Commissioner has access to all relevant documents and material; all persons involved in interception are required by law to cooperate fully with him. He reports at least annually to the Prime Minister, and these reports are published. An Investigatory Powers Tribunal exists which considers complaints from the public about interception, and can order appropriate remedies.

20. The Act specifically bars any evidence in court, or any question, assertion or disclosure in legal proceedings, which results from warranted interception or would reveal that warranted interception had taken place. The only exceptions are

- Proceedings before the Investigatory Powers Tribunal
- Proceedings relating to offences under the Act itself (such as illegal interception)
- Certain special closed proceedings (Special Immigration Appeals Commission, Proscribed Organisations Appeals Commission, Control Orders under the Prevention of Terrorism Act 2005). All these cases relate to executive actions, and are civil rather than criminal proceedings to which a different standard of proof and different rules of evidence apply. Intercept can only be introduced in closed session, in which the appellant is represented by a cleared Special Advocate.

21. In all other criminal proceedings where warranted interception has taken place it is the duty of the prosecution to review any relevant intercepted material (including summaries and reports) that still exists at the time, in order to determine what action is required to secure the fairness of the prosecution. If necessary the Crown must disclose the material to the judge, who can, where he is satisfied that the exceptional circumstances of the case require him to do so, direct the prosecution to make an admission of fact. It is never permissible to disclose the material to the defence.

22. Only material intercepted under a UK interception warrant is affected by this bar. It does not apply for example to material intercepted in a foreign country under that country's law; to a telephone conversation recorded with the consent of one of the participants; or to a telephone conversation recorded by a hidden microphone not connected to the telephone. In all of these cases the material may be adduced as evidence, and is subject to the same disclosure rules as any other relevant material.

23. The Government has recently proposed adding to the list of exceptions closed appeals against Treasury orders freezing the assets of terrorists. These appeals would be conducted in the same way as Special Immigration Appeals Commission and other special closed proceedings. Separately, they

propose to amend RIPA so as to allow intercept to be used in coroners' courts subject to certain limitations – see Chapter IV.

STRATEGIC CAPABILITY

24. Interception in accordance with the UK's legal framework provides a major strategic capability, which is available for use by both the UK's intelligence agencies and its law enforcement agencies. ***

25. GCHQ passes intelligence *** to the other intelligence agencies, and the law enforcement agencies, as a result of tasking or to meet their stated requirements. All the agencies can themselves carry out warranted interception of individual targets in the UK through the service providers and an infrastructure managed on their behalf by the National Technical Assistance Centre (NTAC, since 2006 part of GCHQ).

26. Both internationally and domestically, interception has to cover as far as possible all the different media that a target can use. The number of different media is increasing rapidly, as described in the section on New Technology. ***

INTELLIGENCE USE

27. Interception by the intelligence agencies makes significant contributions to Counter Terrorism (CT) and military operations both in the UK and abroad. *** GCHQ provides support to all Security Service's priority 1 ("threat to life") terrorist investigations, and many of those at priority 2. It has recently had significant success ***, and has provided a number of new leads for Security Service. In addition SIS works closely with the Security Service to pursue leads overseas to terrorists active in the UK; many of these leads originate from interception.

28. ***

29. ***

30. ***

LAW ENFORCEMENT USE

31. Interception is available to all UK police forces and certain other bodies responsible for investigating serious crimes. In England and Wales it is carried out on behalf of all police forces by the Serious Organised Crime Agency (SOCA) which also makes extensive use of this capability for its own purposes; in Scotland by the Strathclyde Police on behalf of the other Scottish police forces; and in Northern Ireland by the Police Service of Northern Ireland. All these forces use interception to investigate serious and organised crime, as well as to counter terrorism (where they work very closely with the Security Service). In addition, the Metropolitan Police (for public order purposes) and HM Revenue & Customs (to counter revenue crime) have

independent facilities, however the bulk of Metropolitan Police interception is provided by SOCA.

32. All these bodies use interception to provide intelligence on the crimes and criminals they are concerned with. SOCA told us that interception, together with communications data, is the single most powerful tool for responding to serious and organised crime. This is because

- It carries very low risk of putting police officers in danger or warning the suspect of police interest in him;
- It is flexible and uniquely easy to put in place quickly;
- It is less costly and less intrusive than for example covert entry, surveillance or eavesdropping;
- It can help ensure the safety of law enforcement personnel; and
- It can provide excellent intelligence of criminals' plans, allowing law enforcement to prevent serious crimes from occurring as well as to collect evidence of crimes being committed.

For these reasons very few major criminal investigations do not involve interception.

33. ***

34. Interception has contributed to a large number of arrests, recoveries of firearms, and seizures of drugs and cash. ***

35. ***

36. ***

37. Very similar evidence was given by other law enforcement bodies across the UK, including the Metropolitan Police, and the Associations of Chief Police Officers in England and Wales and in Scotland. Only the Serious Fraud Office (SFO) regards interception as of limited value to its current work, because most of its investigations are carried out after the event, when suspects are unlikely to be discussing a fraud which has been completed. However the SFO is dealing increasingly with live cases, and it believes that interception would be of value for these.

38. Even though the intercepted material cannot at present be used as evidence, it is of great value as criminal intelligence. The information it provides enables police to intervene at the key moment when and where there is clear evidence of an offence. It can reveal criminals' plans, allowing police to disrupt the plan before it can

A Category A prisoner, serving an indefinite sentence for armed robbery, escaped from prison. Communications data enabled the identification of a mobile he was using. Interception showed that he and associates were planning an armed robbery to raise funds to make good his escape. It revealed where he was staying under a false name. The prisoner was arrested and returned to prison. The intended armed robbery never took place.

be put into practice. Or an intercepted message may give the go-ahead for the crime itself, allowing the police to be in position to arrest the criminals red-handed.

Interception of a highly professional international group involved in trafficking Class A drugs revealed the intention to import a large consignment. As the plan developed it identified individuals recruited to transport and receive the drugs. The intercepted calls were in coded language which could have been attributed to legitimate activity. The group evidently had a lot of knowledge of covert techniques, but not enough understanding of how they are used to provide effective security.
Continued interception revealed new timings for the importation and travel arrangements for those involved. This enabled officers to observe the collection of the drugs, arrest two of the principals, and seize 20 kilograms of heroin, over 20 firearms, and over 1000 rounds of ammunition.

39. Interception after a crime has been committed can lead police to the suspects and allow them to recover the proceeds.

Interception of two men suspected of being involved in a recent major armed robbery confirmed their involvement and showed how they were responding to the police investigation. It also identified others involved, who were themselves intercepted. The speed at which coverage was put in place prevented the robbers from removing the proceeds overseas. It gave opportunities to gather physical evidence and allowed several arrests and the recovery of substantial sums of money.

40. Interception is of particular value in dealing with the substantial number of kidnaps for ransom or revenge within the criminal community. For obvious reasons such kidnaps are never reported to the police. But for interception of those involved, the police would not even know that a kidnap was happening. With interception the police are regularly able to intervene to save the victim's life, or even to prevent the kidnap from ever taking place. Since the victims are usually unwilling to testify, these crimes seldom result in prosecutions. As a result of interception and other tools no life has been lost in such a kidnap since 1999.

In 2007 a person contacted police reporting the kidnap of a friend over a debt. A third party was apparently negotiating in isolation and refusing to cooperate with the police. A further party was also negotiating without cooperating fully with the police. The situation was further complicated by direction from members of the criminal group abroad. Interception over several days confirmed that the hostage, although injured, was alive. It allowed police to control the developing situation to the point where a significant sum of money was paid and the hostage released. This triggered the arrest of all involved in the kidnap, and the recovery of the ransom.

41. These results owe much to the flexible and efficient way in which interception can support operations with minimal bureaucracy. There is very close cooperation between those monitoring the intercepted lines

– often in real time – and those commanding the operational response. Lines can swiftly be set up or closed as operational priorities change.

COOPERATION BETWEEN INTELLIGENCE AND LAW ENFORCEMENT

42. The whole interception community – law enforcement as well as intelligence – benefits from *** the shared tools and techniques that the intelligence agencies have developed. This close co-operation is not found in other comparable countries including the USA which have a strategic intelligence capability ***. When hostages have been taken the police craft a dynamic response around a wide variety of covert collection techniques, relying critically on support from the intelligence community *** to provide information on the capability and intent of the hostage takers, to mitigate risks to life, and to identify opportunities for the safe release of the hostages.

SUPPORT FROM COMMUNICATION SERVICE PROVIDERS

43. Under RIPA, Communications Service Providers in the UK may be required to provide, at public expense, an adequate interception capability on their networks. In practice all significant providers do provide such a capability. ***

44. Increasingly communications services (especially over the Internet) can be provided by companies based outside the UK's jurisdiction. Existing UK providers could, at little cost or risk to their operations, move some or all of them offshore. In some, but not all, such cases adequate access can be obtained through international agreements such as the EU Mutual Legal Assistance Convention. But in other cases legally mandated access is simply not possible.

45. ***

CONCLUSION

46. As illustrated above, interception is a critical component of the UK's strategic intelligence capability. **The Review is confident that this capability is essential for national security and so must be retained and protected.** We regard it as our starting point that any scheme for the use of intercept in evidence in criminal cases must respect this strategic imperative.

47. In addition to this strategic use, interception is used today in a very effective and efficient way to investigate terrorists and serious organised criminals, and to assist with their prosecution and conviction. We accept the principle that all classes of evidence should be admissible unless there are compelling reasons against; and there is an obvious practical disadvantage in the present prohibition on the use as evidence of material which might allow the conviction of individuals who may now go free or have to be restrained by other means which have proved controversial. On the other hand we have had to consider how much of today's use of interception might be lost as a result of capabilities being revealed in court, new requirements imposed to

support evidential use, and cooperation with intelligence agencies and with Communications Service Providers made harder. It is on that balance of advantage that the Review bases its conclusions.

CHAPTER III - POTENTIAL USE AND BENEFIT OF INTERCEPT AS EVIDENCE

PRINCIPLES

48. In principle every court should have available to it the best evidence available which will determine whether the accused is guilty or not. The accused's own words, intercepted and played to the court, can obviously be extremely powerful evidence. In particular, they can give the jury an insight into his intentions and state of mind at the time the alleged crime was being committed, an area where other direct evidence may be hard to find. The evidence provided by interception will be especially well-suited to proving charges of conspiracy, where the nub of the offence lies in what a group of individuals say one to another. **We agree with the principle that the best evidence should be made available to the court, unless there are compelling reasons why a particular class of evidence should not be used.**

49. We have also heard powerful evidence that the state should manage terrorism through strict use of normal legal process. That implies prosecuting and convicting terrorists wherever possible; other quasi-judicial measures, falling short of prosecutions, should ideally have no place. More generally better prosecutions are needed across the board, for criminals as well as terrorists. Therefore it is the Government's job to ensure that all possible evidence can be used to ensure that the guilty are brought to trial and convicted. If that is done, the argument goes on, the need for exceptional measures such as Control Orders and lengthy pre-charge detention will be significantly reduced or even disappear, and public confidence in the criminal justice system will be maintained.

EFFECTS ON TRIALS

50. There is strong evidence from experience abroad that the availability of intercept as evidence can significantly influence the course of a trial. Some defendants, confronted with recordings of their own words, may well realise that their case is hopeless, and decide to plead guilty. They may even choose to provide active assistance to the prosecution, for example by giving evidence themselves against their criminal bosses and so enabling the conviction of the latter, or by providing convincing evidence of the real meaning of suspicious conversations in which they took part. It was by using intercept in these ways that the US authorities – much helped by the ability to 'plea bargain' there – have recently been able, for the first time, to convict the heads of all 5 New York mafia families (see Chapter VII). It is of course not possible simply to transfer unchanged to the UK methods that are used successfully in other jurisdictions, where the legal background is different, but the evidence of success there cannot be ignored.

51. The Crown Prosecution Service (CPS) expects a similar effect if intercept as evidence is introduced in the UK. It foresees savings in court time through more early guilty pleas, and fewer abortive trials. The Serious

Organised Crime and Police Act 2005 gave powers to grant a suspected offender immunity from prosecution, or to pass a reduced sentence, in return for the offender's written agreement to provide assistance. CPS experience is that such agreements are greatly facilitated when clear evidence is available at an early stage; they believe that intercept evidence would be particularly powerful, and could be crucial in achieving agreements.

EFFECTS ON PROSECUTIONS

52. While everyone can agree that using intercept as evidence would result in some additional successful prosecutions, we have heard very different views on the scale of the increase and the sorts of cases involved. Those with experience in interception have emphasised that the vast majority of communications between serious criminals or terrorists are scrappy, highly allusive, and often deliberately disguised as legitimate conversations. Regardless of language, they make extensive use of dialect and slang. Clear, understandable exchanges that plainly inculpate those involved are very much the exception. For the rest, much interpretation – as well as translation in many cases – is needed to reveal what the exchange is really about. This need is particularly acute where multiple media are used – see Chapter VI.

53. A substantial piece of work was carried out as part of a previous review of this subject in 2003-04, which took a considerable number of real cases in which interception had been used, examined whether the actual intercept obtained would have been of evidential value, had it not been barred from use, and estimated the effect on the outcome. Its conclusions were that intercept would result in 25-30 additional convictions each year across the UK, mainly of second and third tier organised criminals (ie not the most important targets). It concluded that few additional convictions of terrorists or first tier organised criminals would be obtained, on the grounds that they generally observe good communications security and avoid inculpating themselves over media that can be intercepted.

54. These conclusions have been criticised in evidence to this Review. It is suggested that if intercept were available as evidence, listeners would be more alert to inculpatory conversations of evidential value. Where the intercepted conversations were inconclusive, other evidence would have been sought to resolve the point. We accept that there is force in these criticisms, which are supported by the successful use in UK courts of foreign intercept (which is exempt from the bar on use as evidence) and eavesdropping, as well as by the use of intercepted material in Control Order and Special Immigration Appeals Commission proceedings.

55. But there are also considerations that pull the other way. For example, the 2003-04 work was based on monitors' notes of the intercept, rather than the recordings themselves; a jury might not be convinced that the monitor's interpretation of the spoken words was the correct one. Further it assumed that all available intercept would be used as evidence: in reality the Crown may decide not to adduce certain intercept on grounds such as exceptional

sensitivity or the risk to other, more important, cases to which the same intercept might be relevant.

56. As part of this Review, the Metropolitan Police have reviewed cases involving interception during 2006-07 in which charges were discontinued or failed to result in conviction. They concluded that intercept as evidence might raise the conviction rate in cases involving interception (excluding those still awaiting trial) from 88% to 92%.

57. Other evidence supports these views:

- ACPO considered a number of cases, in two of which intercept could have been used as supporting evidence.
- The Serious Fraud Office (had the law allowed) would have used intercept as evidence in a particular insider-dealing conspiracy case.
- The Northern Ireland Public Prosecution Service consider that removal of the bar could assist considerably in a small number of important cases, either helping to meet the test for prosecution or strengthening prosecution cases that already met the test.

58. We have also seen a recent review of nine current or former Control Order cases, conducted by independent senior criminal Counsel *** for the Home Office. It concluded that the ability to use intercepted material in evidence would not have enabled a criminal prosecution to be brought in any of the cases studied - in other words, it would not have made any practical difference. In four cases, Counsel concluded that such intercepted material as exists, even if it had been admissible (including the assumption that it could be made to meet evidential standards), would not have been of evidential value in terms of bringing criminal charges against the individuals in question. In the other five cases, although Counsel assessed that there was intercepted material capable of providing evidence of the commission of offences relating to encouraging, inciting or facilitating acts of terrorism (as opposed to the direct commission of terrorist or other offences), he stated that *"it is clear to me that in reality no prosecution would in fact have been brought against these five men"*. This was because deploying the crucial pieces of intercepted material as evidence would have caused wider damage to UK national security (through, for instance, exposing other ongoing investigations of activity posing a greater threat to the public, or revealing sensitive counter-terrorism capabilities to would-be terrorists) greater than the potential gains offered by prosecution in these cases.

CONCLUSION

59. No one has asserted that evidential use of intercept would bring about a major increase in successful prosecutions. **The limited evidence available suggests that there would be a modest increase in successful prosecutions, at different levels of seriousness, as a result of the use of intercept as evidence.** We have not seen any evidence that the introduction of intercept as evidence would enable prosecutions in cases currently dealt with through Control Orders.

CHAPTER IV - RISKS

60. Against the potential benefits of making intercept material admissible in court must be weighed a range of risks, including risks to the current use of intercept as an intelligence and law enforcement tool.

61. There are a series of inter-woven legal, technical, operational, and organisational risks that need to be considered when judging whether an intercept as evidence regime could and should be devised. In addition, there are various resource implications, which we deal with separately in the following chapter.

LEGAL RISKS

62. Any intercept as evidence regime would have to be compatible with the European Convention on Human Rights. In particular it would have to ensure a defendant's right to a fair trial, as set out in Article 6, and everyone's right to private and family life, as set out in Article 8. If the statutory bar on use of intercept product as evidence were lifted, any potentially exculpatory material would, under CPIA[2] rules and to ensure 'Equality of Arms', need to be examined and (if found to support the defence case or undermine the prosecution case) disclosed.

63. Although the prosecution would be able to apply for Public Interest Immunity to protect against the disclosure of sensitive techniques and capabilities, this protection is not absolute. There is not only the risk of a quixotic ruling by an individual judge. In each case, the trial judge is obliged to ensure the defendant's right to a fair trial. Even when considering a Public Interest Immunity application, judges are obliged to look only at the circumstances of the case in question, and to disregard any wider consequences of their decision.

64. A number of operational and organisational risks flow from these legal requirements.

RISK OF DISCLOSURE

65. Any disclosure of interception capabilities could have a profound impact on national security, by encouraging a wide range of targets (not only criminals but also terrorists and other individuals of intelligence value) to change their behaviour in ways that would make them more difficult to investigate in the future. This can happen (and has happened in practice) simply in consequence of the successful interception of a particular call becoming known – the target will of course know in what way that call was made. It will not be enough to protect the techniques that allowed the call to be intercepted. As a result such a call could not be adduced as evidence.

***

[2] Criminal Procedures and Investigation Act 1996

66. The existence of an official capability to intercept telephone conversations is not a secret. However, beyond that basic fact there has never been confirmation of what communications can be intercepted (and how) and what not (and why not). It is often suggested that criminals "know" what the government's capabilities are. In reality, they do not know; they often presume based on partial information, experience overseas where conditions are different, and rumour. Some of their presumptions are right, others wrong.

67. Many intelligence and law enforcement targets take pains to avoid interception or obfuscate their communications. At present they cannot know which of their efforts are successful and which not. ***

68. The damage from disclosure of capabilities in criminal cases would not be limited to law enforcement. Targets that threaten national security (including terrorists, arms traffickers and spies) have access to the same communications as criminals, and would quickly draw their own conclusions from revelations in the courts.

INTER-AGENCY COOPERATION

69. The intelligence agencies have a duty to protect their sensitive techniques and capabilities ***, which are vital for securing the UK's national security. At present they are able to – and do – use these techniques and capabilities very widely in support of law enforcement. *** Intelligence provides significant benefits to the UK through the generation of leads that result in successful terrorism and serious crime prosecutions, as well as the prevention of such acts through disruption operations (the value of this current cooperation is set out in Chapter II). The use of these techniques will become even more important as new technology is introduced (see Chapter VI).

70. It is argued that, under a new regime that made intercept useable as evidence, supporting law enforcement in this way might put these sensitive techniques and capabilities at risk of exposure in court. Because of the serious damage such exposure could cause to intelligence capabilities across the board, and in particular to their own relations with cooperating agencies abroad, the UK agencies might be unable to continue with the present level of support to law enforcement. Such a reduction in cooperation could have a profound impact on law enforcement agencies' ability to combat serious crime and terrorism in the UK.

COMMUNICATION SERVICE PROVIDERS

71. The UK's capabilities are dependent on the partnerships that have been developed with Communications Service Providers (CSPs). *** The CSPs have made it clear to us that the bar on intercept as evidence has been a critical element in building up that partnership. ***

72. If CSPs were to reduce their cooperation, this would seriously affect the UK's strategic intelligence capability ***. It would also impact on the

tactical ability of law enforcement agencies to combat terrorism and other serious crime in the UK. ***

73. The CSPs, intelligence and law enforcement agencies are also concerned about the risk to individuals who are involved in interception ***. The CSPs are very mindful of their duty of care to their staff. ***

74. If it were decided to introduce an intercept as evidence regime, the Government would need to create confidence among the CSPs *** and to explain how any potential risks were being mitigated.

INTERNATIONAL RELATIONSHIPS

75. Any increased risk of disclosure could also harm international relationships ***.

76 ***

TECHNOLOGY CHANGE

77. The impact of technology change and the resulting risks could change the benefit versus risk equation. *** This issue is dealt with in greater detail in Chapter VI.

LEGAL CHALLENGE

78. Any legal challenge to an intercept as evidence regime could result in a delay of a number of years, before court interpretation of the relevant law was clarified. There would certainly be some degree of uncertainty concerning the full risks and resource implications when intercept as evidence was first introduced, as it would not be possible to predict judicial responses to the new regime and how the relevant jurisprudence would develop. However carefully the new legal regime would have been designed to protect vital national interests, jurisprudence (nationally and in Strasbourg) may take a different path from that predicted.

79. Varying degrees of uncertainty clearly accompany many new legal provisions, but the impact of the uncertainty needs to be factored into the cost/benefit analysis and the Review's final judgement. Any legal model proposed should be robust enough to minimise this risk, and be accompanied by credible Government assurances that any possible consequences will be effectively addressed.

NORTHERN IRELAND

80. Discussions with and written submissions from Northern Ireland law enforcement agencies highlighted a number of particular risks that they would face from the introduction of IaE. ***

81. We have been told that the use of non-jury trials has been one of the factors leading to more stringent disclosure requirements in Northern Ireland courts than in England and Wales. ***

82. ***

83. In addition, public enquiries have wide-ranging powers to order disclosure, that cannot be fettered by public interest immunity, which would need to be considered. The Police Ombudsman for Northern Ireland may also, in accordance with section 66 of the Police (Northern Ireland) Act 2000, require that the Chief Constable of the Police Service of Northern Ireland provide him with any information in his possession, regardless of its nature or potential sensitivity. While the Police Ombudsman is confident that he has appropriate measures in place to protect sensitive information, this Review will need to take due regard of these powers. **Because of these particular risks, we recommend no change to the current legal regime for interception in Northern Ireland.**

SCOTLAND

84. There are also a number of particular issues and risks concerning the implementation of intercept as evidence in Scotland and how the Scottish legal system would have to be adapted. The interception of communications is listed among the reservations in Schedule 5 to the Scotland Act 1998 so that Westminster retains competence, although Scottish Ministers are authorised to sign interception warrants relating to serious organised crime. The law of criminal procedure is however devolved and Scottish Ministers and the Scottish Parliament have competence to deal with such matters as the use of intercepted evidence in the context of a Scottish prosecution. The Scottish Government also have devolved responsibility for policing. We have therefore had to consider the impact that the mixture of reserved and devolved competences would have on making any changes in Scotland.

85. A particular issue in Scotland is that any intercept as evidence model likely to be considered would probably rely on some form of Public Interest Immunity, entailing a combination of pre-trial *ex parte*[3] hearings or other methods of protecting sensitive material, consistent with the procedures set elsewhere in the UK by the Criminal Procedures and Investigation Act 1996. There are currently no provisions for PII in Scotland, although *ex parte* hearings can be held. In the absence of PII, the risks of disclosure in Scotland would be significantly greater than in England and Wales. A review on the 'Law and Practice of Disclosure in Scotland' has recently been completed by the Rt Hon Lord Coulsfield. He has recommended that legislation should provide a system of Public Interest Immunity hearings in Scotland along the lines of those in England and Wales. The Scottish Government will be consulting shortly on Lord Coulsfield's recommendations and legislation may follow. **We therefore recommend no change to the**

[3] *Ex Parte* – closed hearings in the absence of the other party

current legal regime for interception in Scotland until new legislation is in place and its potential impact has been assessed.

CIVIL PROCEEDINGS

86. Although this Review has largely focused on whether a regime to allow the use of intercepted material in criminal court can be devised, we have also considered the particular risks that would result in making intercept product admissible as evidence in civil proceedings. Repeal of section 17 of RIPA would open up the possibility of using intercept material in civil proceedings, including civil proceedings against the State (eg employment tribunals). In criminal proceedings, if the disclosure of damaging sensitive material is otherwise legally unavoidable, the prosecution has the option of discontinuing the prosecution. In civil cases, where such damaging disclosure to the plaintiff is otherwise legally unavoidable, the only practicable way of discontinuing proceedings would be to pursue a settlement. However, there could well be instances where the plaintiff would be more interested in gaining disclosure of the sensitive material and would not settle, or where his lawyer thought that by pursuing the issue of intercept, the State would be under greater pressure to settle on favourable terms. There would also be cases where the State was not a party to the case, but where one of the parties claimed that there was relevant intercept evidence that should be disclosed; in these instances the State would not have the option of withdrawing from the case or settling.

87. Another significant difference between civil and criminal procedures is that in a civil trial it is only the judge, rather than a jury, who decides both the facts and the law. In a criminal trial it is beneficial, to ensuring a fair trial, for a judge to have oversight of material withheld from the jury (eg on a PII application). However, in a civil case if the material undermines the case of a party from whom it is being withheld, then there is a risk that the trial judge will be prejudiced by seeing it, and if he were to rule it inadmissible the result would be unfair to the other party, whose case could have been undermined in the eyes of the judge by evidence which they had not seen.

88. **Because of the particular risks involved in introducing intercept as evidence in civil proceedings, we recommend that any change to the current legal regime for interception in the civil courts only be considered following successful change in criminal proceedings.**

89. While our Report was in the final stage of drafting, the Home Secretary announced her intent to amend RIPA so as to allow intercept to be used at Coroners' Inquests subject to certain limitations and on the basis that there would be no jury. This announcement came too late in our consideration for us to investigate or assess it without delaying our Report.

RISK TOLERANCE

90. The Review has considered at some length the extent to which it is reasonable to tolerate these risks as a reasonable price for the benefits that

intercept as evidence would bring. In this respect, the risks are by no means equal. **We have concluded that any material risk to the strategic capability of the UK's intelligence agencies would be unacceptable.** This is entirely consistent with our terms of reference requiring us to treat national security as an "overriding imperative". In our view it would be wholly irresponsible to move to any legal model that clearly put our national Sigint capability (and the relationships with other countries *** that underpin it and make it possible) at any significant risk. Our analysis of candidate legal models (see Chapter VIII) takes that as its starting point.

91. Other risks are however not of this kind, and it may be reasonable to accept a degree of uncertainty, while avoiding the danger of unfairness to a defendant. Our consideration has enabled us to frame what we consider to be the prerequisites for any legal regime to be considered operationally workable (in effect incorporating what the Review judges to be the appropriate tolerance of risk in introducing a regime that uses intercept as evidence).

REQUIREMENTS FOR INTERCEPT AS EVIDENCE TO BE OPERATIONALLY WORKABLE

- The intercepting agency shall decide whether a prosecution involving their intercepted material shall proceed.
- Intercepted material originating from the intelligence agencies shall not be disclosed beyond cleared judges, prosecutors, or special (defence) advocates, except in a form agreed by the originator.
- Material intercepted (by any agency) through the use of sensitive Sigint techniques shall not be disclosed unless the Secretary of State is satisfied that disclosure will not put the capability and techniques at risk.
- No intelligence or law enforcement agency shall be required to retain raw intercepted material for significantly more or less time than needed for operational purposes (which may include using the material as evidence).
- No intelligence or law enforcement agency shall be required to examine, transcribe or make notes of intercepted material to a substantially higher standard than it believes is required to meet its objectives (which may include, but are not limited to, using material as evidence).
- Intelligence and law enforcement agencies shall be able to carry out real time tactical interception in order to disrupt, interdict or prevent terrorist and criminal activity, as effectively as they do now.

- Law enforcement agencies shall be able to use interception to provide strategic intelligence on criminal enterprises, and retain the intelligence sometimes for a number of years, regardless of the progress of specific criminal cases. Interception from the same lines may serve both tactical and strategic purposes; if it does, it shall be handled in a manner appropriate to both.

- Intelligence agencies must be able to support law enforcement by carrying out interception, for 'serious crime' purposes, of targets nominated by law enforcement, and to provide the product or reports on it to those agencies. Anything so provided shall be subject to the same disclosure obligations as other intelligence intercept.

- At trials (whether or not intercept is adduced as evidence) the defence shall not be able conduct successful 'fishing expeditions' against intercept alleged to be held by any agency.

92. These requirements provide the operational parameters that any Intercept as Evidence regime would need to meet, along with being ECHR and Common Law compatible, and have set the context for the consideration of legal models in Chapter VIII, and for our conclusions in Chapter IX.

CHAPTER V - RESOURCE IMPLICATIONS

INTERCEPTING AGENCIES

93. There are several reasons why intercepting agencies may need extra resources if intercept were adducible as evidence. The main ones are:

- To retain the original intercepted material, and any notes or transcripts, until the criminal process is completed (whereas for intelligence purposes it would be deleted after a short time)
- To assure the integrity of retained material and any processing it undergoes (so that a court can judge that it accurately represents what was in fact sent, and has not been tampered with in any way)
- To monitor, transcribe or translate more of the material, or in greater detail, than is required for intelligence purposes
- To provide an effective guide to the content of what would be a larger quantity of retained material, so that the prosecution can identify anything that might undermine their case or support the defence (as required by the Criminal Procedure and Investigations Act 1996).

Most of these potential requirements depend on what legal model is adopted, and what that would mean in practical terms – which may be determined as much by decisions in the courts as by legislation. The size of the requirement for a particular agency will also depend on that agency's current practice, by no means uniform between agencies. As a result there are big uncertainties in estimating the new resources required, and there are differences between estimates provided by different agencies.

94. ***

95. ***

96. ***

97. ***

98. ***

99. ***

100. ***

101. In addition to all this the new systems being developed to carry out interception in the IP era would have to be brought up to appropriate evidential standards. As noted in Chapter VI, the cost – and indeed practical challenges – of doing this are unclear, but are likely to be substantial.

102. The intercepting agencies express further concerns. Many terrorist and criminal targets communicate in obscure languages and dialects, requiring the intercepting agencies to recruit transcribers and monitors who have sufficient knowledge of these languages. ***

103. Although there would be less of a direct impact for other departments and agencies such as SIS, Defence Intelligence and FCO, any diversion of GCHQ or Security Service capability would adversely affect them and the Government Departments which task them, by reducing the effort available to meet their requirements. They would be particularly concerned if the limited number of transcribers and monitors of obscure languages were diverted from supporting critical overseas CT, foreign policy, counter-espionage, force protection or counter-kidnapping operations.

104. If for whatever reason new resources were not made available, or if the required extra staff could not be found, the inevitable consequence would be a reduction in the agencies' capability. The Association of Chief Police Officers predicts that an evidential regime would result in a dramatic reduction in capacity, which would impact significantly on the potential for interceding in 'loss of life' situations such as kidnaps and threats to kill. It believes that the damage, particularly in counter-terrorism, would not be compensated by the limited benefits of being able to adduce intercept as evidence. The Metropolitan Police, the Association of Chief Police Officers in Scotland and the Police Service for Northern Ireland make similar points.

THE CRIMINAL PROCESS

105. Intercept as evidence will clearly have some significant resource effects on the criminal justice system:

- The availability of intercept evidence may sometimes obviate the need for other, more costly, investigative techniques such as surveillance.
- The weight of intercept evidence may persuade some defendants to plead guilty, so saving much of the cost of a trial.
- On the other hand some trials may need to take account of more evidence, and so will take longer to prepare for and will run for longer.

106. It is however very hard to predict how effects that will increase costs to the criminal justice system (apart from the increased costs to the intercepting agencies covered in the previous section) will be balanced against those that will save costs. The Director of Public Prosecutions for England and Wales has told the Review that savings will in his view at least balance any increases in this area. Other witnesses believe that the greater body of evidence provided by intercept product would normally increase the length and cost of trials. The likely resource impact on the criminal process could only be confidently assessed by running scenarios of actual cases based upon a detailed understanding of a specific legal regime.

CHAPTER VI - NEW COMMUNICATIONS TECHNOLOGY

WHAT IS IT?

107. Over the next several years the worldwide public telecommunications network will undergo a profound change. Hitherto almost all telephone networks have been circuit-switched: whenever a call is made the provider has set up a dedicated circuit (a combination of wires, channels within fibre optic, microwave or satellite trunks, and radio links to individual phones) which connects the callers. For as long as the call lasts the callers have exclusive use of this dedicated circuit. While other services than ordinary telephony (such as data) may be available, they are generally under the control of one of a small number of suppliers, who provide both the service and the underlying network, and do any necessary processing.

108. Within the next 5 years we expect that most communications in the UK will instead be delivered using Internet Protocol (IP)[4]. There are strong commercial forces driving this revolution, and unlike the so-called 'Telecoms Bubble' in the late 1990s these plans are well founded. The same economic forces will drive all Communications Service Providers (CSPs), in the UK and abroad, to make similar changes to their networks, albeit not always in the same timescale.

109. This process is being driven by – and in turn will enable – a rapid predicted growth in the volume of communications. The Home Office have gathered data from various sources, which predicts that the number of discrete communications events per year in the UK will nearly double in ten years, from some 230 billion in 2006 to nearly 450 billion in 2016. The bulk of that growth will be in messaging and non-voice communications using IP – the trend for voice communications (fixed and mobile) is relatively static.

110. In the UK this process is exemplified by British Telecom's move to its 21st Century Network, in which it is investing £10 billion over the period 2007-2011. On the core network itself all traffic will be IP based from the start; there will be no differentiation between voice and data. This IP network will potentially allow its customers to access any communications service (whether provided by BT or not) at broadband speed from any device, and will link fixed and mobile networks. For BT customers only requiring a plain voice telephony service, the signal will initially be converted from IP by BT before entering the home, but it is expected that existing telephones will (over a longer period) be replaced with cheaper IP devices able to exploit the vast range of available services. Then all customers will access the core BT network through a broadband link, regardless of the service they choose to pay for.

111. The migration to IP will result in two fundamental changes.

- Firstly CSPs will be carrying all voice (both mobile and fixed-line) using IP based networks. Many users will not consciously choose to move to

[4] The international standard used for delivering material across the Internet.

Voice over IP, and may be completely unaware they have done so, but it will happen to them none the less.

- Secondly most communications devices will have high-speed internet access provided as standard. This will enable people to make use of any of the thousands of services available on the internet, provided by suppliers anywhere in the world or even by users cooperating amongst themselves. The processing that makes that possible will be done by a mixture of the suppliers' servers (which may well be located offshore) and the customer's own equipment. It is becoming easy for a user to move between a number of services, provided by different suppliers, in the course of a single call – see the example in the box.

During its investigations the review team was given the following real-life example of the type of multi-thread communication that occurs naturally with modern communications systems.

Three friends Ian, Michael, and Stuart are planning a trip to the cricket. Stuart texts Ian from work to ensure he will be at his computer a little later to organise the trip. He then goes home and turns on his computer. He sends an Instant Message to see if Ian is online, which he is. Both then log onto their favourite Voice over IP (VoIP) package and begin discussing the trip. They quickly realise it would be easier if they could both see the fixture list, so Stuart e-mails to Ian a link to the cricket club's web-site. This fails, so instead he posts the link to a web forum they both use.

They carry on their discussion and agree which match they wish to see. Michael is also online but does not have the same VoIP package so can't join in the conversation. However he and Ian are playing the same on-line computer game, and so use the in-game text-based chat function to discuss the details, Ian acting as a relay between Michael and Stuart. Finally all agree that Ian will buy the tickets. The others use an online bank (PayPal) to send the money to him. This in turn generates confirmation e-mails.

So over the course of 30 minutes the three friends have used half a dozen different communications methods, not with any intention to conceal their activities but because it's a convenient and natural way to use the technology.

112. Many of these standard services offer their users anonymity and security - although users often may not be aware of this. Anonymity may result from embedded security features, or simply from the weak registration typical of the many free services available – users may not even need to identify themselves before using them, and even if they do, it is usually easy to give a false identity.

WHAT DOES IT MEAN FOR INTERCEPTION?

113. Some witnesses, while of course accepting that these changes are happening, argue that they are not relevant to the question of using intercept as evidence. This, they suggest, is a matter of principle, not to be driven by the technology of the day. We do not believe it is as simple as that; an intercept as evidence regime must be workable and practically useful within the technological framework which actually exists, and increasingly that will be IP.

114. Circuit-switched telephony lends itself to a simple model of interception. Once the system has recognised that a call to or from a target

telephone is being set up, any part of that circuit can be accessed and the whole contents of the call copied to the intercepting agency. In times past that was done by connecting a recording device direct to the wires the target was using. Nowadays more sophisticated methods are used ***. But the principle is the same. ***

115. This model breaks down when individual circuits are replaced by IP networks. *** some interception will still be possible through the switch by which the particular target is connected to the IP network. But access even there will typically only allow interception of the raw IP data going to that target's location; subsequent processing is then required to interpret and separate specific communications, if the interceptor is to stand any chance of making sense of them. ***

116. The problem becomes all the harder when the predicted growth of the overall telecommunications business are taken into account. The needle the interceptor is searching for will be hidden in an ever larger haystack.

117. There are no recognised standards for the services that will be offered, so almost every different service will require its own bespoke processing capability. Resources will never be sufficient for this to be possible; instead the authorities will need to prioritise, and put in place processing for those services which their targets already use or are likely to use in the future. This necessary prioritisation makes the interception system vulnerable to unforeseen changes in target behaviour. There will inevitably be gaps in capability; if targets become aware of them, it will be quick and easy for them to move away from services that the system can process, and instead use services it cannot. Then for a period interception will be unable to reach these targets, until new processing can be devised and put in place. At this point the cycle can start all over again.

118. To meet this challenge the Home Office is leading a Government-wide Interception Modernisation Programme ***. The Programme has been set up, and is beginning to design potential solutions, on the basis of existing law, under which intercepted material is not available for use in evidence. The scale of change required to make its product useable as evidence is not known, but delays, increased risk and increased cost seem likely.

119. ***

120. There are a number of practical difficulties with using Internet Protocol material as evidence.

- Putting multiple inputs together will demand a degree of sophisticated analysis by the intercepting agency, which may not be easy to explain to a jury. This will of course be over and above interpreting the targets' use of veiled and allusive speech, obscure dialects etc.
- If any one of those inputs is missing ***, it will be easy for the defence to argue that the missing content would provide an innocent explanation of the apparently incriminating contents of the others.
- ***

- If it becomes known, from one criminal case, that a particular service can be exploited by the intercepting agencies, other criminals will easily be able to move to different services (from the wide choice available through the Internet) which they believe are more secure. This will quickly result in the loss of useful intercept ***.
- In the same way, if it becomes apparent that a particular service cannot be exploited, it will be easy for criminals and terrorists to make deliberate use of it. They will not need to know why that service is unexploitable.
- Some services will be (or will be alleged to be) vulnerable to hacking or spoofing. It will be possible for the defence to argue that incriminating material was falsified (whether by law enforcement or by third parties), and hard for the prosecution to rebut such arguments. While voice identification techniques (though far from infallible) can be used to prove that a telephone call was indeed made by the target, it will be much harder to prove that an email or other non-voice communication was from the purported sender.

121. Recognising that this challenge is by no means limited to the UK (though it may happen sooner here), we have tried to establish how other countries plan to address it. We have found it hard to get accurate data. It appears that most countries plan to rely for law enforcement purposes on software likely to be built into IP switches – even though such access will allow at best partial interception of the many services which will be available to their targets, not all of them provided by domestic suppliers. We are confident that such a simplistic approach will be inadequate for the UK, whether or not intercept is used as evidence.

122. To the extent that other countries have more sophisticated access (invariably through their intelligence agencies), we do not expect them to use the product evidentially. This distinction is already clear in the US ***.

CONCLUSION

123. The advent of new technology will require wide-ranging and very expensive changes to the UK's interception systems. All interception, even of seemingly simple telephone calls, will have to make use of the same advanced techniques. **To protect these techniques and the strategic capabilities they bring, a significant proportion of IP intercept will not be available for use as evidence.** This requirement has influenced the legal models we have considered – see Chapter VIII.

CHAPTER VII - RELEVANCE OF EXPERIENCES OF OTHER COUNTRIES

124. One of the most regularly made arguments in favour of introducing intercept as evidence, is that the UK is one of few countries that does not allow the use of intercepted material as evidence; with the question being put; "*if other countries can use intercept as evidence safely, why can't we?"*

125. In order to understand whether there were any sound reasons for this apparent anomaly, and to learn any lessons from other countries' use of intercept as evidence and their legal and operational regimes, we gathered material from twelve different countries. We attempted to look beyond how intercept as evidence was allowed for in principle, as set out in statute, to get a sense of the value of intercept as evidence in practice and how they managed the related risks and costs. In order to consider the issues faced by the UK, being a common law jurisdiction which is also subject to the European Convention on Human Rights, we examined a mixture of EU member state, common law and other jurisdictions[5].

126. For each of these countries, we considered:

- Their assessment of the benefits, risks and costs of intercept as evidence;
- The relevance of each comparison to the UK; and
- What each comparison indicated in terms of likely benefit, risk and cost to the UK of introducing intercept as evidence.

127. We have outlined below our analysis of the use of intercept by seven of these countries, namely: France; Republic of Ireland; Netherlands; Spain; Australia; Canada; and United States. The use of intercept by the remaining countries we received material from did not raise any substantial additional issues.

EU COMPARISONS

France

128. The French employ a dual system of intercept, using judicially-authorised interception for law enforcement purposes and administratively-authorised interception for intelligence. The two systems use separate personnel (except for translators) and separate technical systems. They are careful to ensure that any public knowledge by targets of law enforcement intercept does not compromise the use of separate intercept capabilities for intelligence purposes.

129. They view judicial interception as essential for many investigations, in particular to support conspiracy charges, drug and organised crime investigations. A small number of judicial warrants are in force at any time.

[5] Australia, Canada, France, Germany, Israel, Italy, Netherlands, New Zealand, Republic of Ireland, Spain, Sweden, United States

*** Not all recordings are kept, with the examining magistrate responsible for advising the police and selecting which recordings to keep.

130. As is the case generally under the French inquisitorial system, most of the evidence gathering and deliberation is done during the pre-trial phase and the trials themselves are relatively short. As evidence collected is the result of a judicially supervised enquiry[6], evidential material, including intercept, is less likely to be challenged during the trial. There is less cross-examination than in the UK, and defence objections to intercept evidence are rare. It is, however, unusual for convictions to be based on intercept alone.

131. Administrative intercept for intelligence purposes may be authorised by the Prime Minister for the purpose of safeguarding national security, scientific and economic well-being or to prevent terrorism, and is carried out by the French security agency[7]. Although administrative intercept is kept totally separate from judicial intercept, a report derived from such intercept can be passed to an investigating magistrate and form part of a dossier of evidence in a criminal case. It is always unsourced (or attributed to an 'anonymous source'). Such evidence would require corroboration and would not secure a conviction alone. If defence lawyers ask any questions about this evidence, the agencies are not obliged to answer them. It is also possible for administrative interception to lead to judicial interception with the security agencies informing an examining magistrate of their suspicions, allowing the latter to start an investigation using judicial intercept.

132. The French are very clear about the benefits that intercept as evidence brings them and are confident that their use is compliant with ECHR requirements. They have developed a system which enables them to benefit from law enforcement use of intercept as evidence to help secure criminal convictions, whilst enabling separate more sensitive intercept capabilities to be used for intelligence purposes by security agencies.

Ireland

133. The example of the Republic of Ireland is particularly interesting as it is the only other Common Law jurisdiction, apart from Malta, that is also subject to ECHR.

134. The Commissioner of An Garda Síochána, the national police force, may apply to undertake lawful interception under the relevant Act[8] either in connection with an investigation of a serious criminal offence or in the interests of the security of the State (as An Garda Síochána is also the

[6] The examining magistrate (juge d'instruction) is responsible for the collection of evidence to establish the truth

[7] DST- Direction de la Surveillance du Territoire

[8] The Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993

security service[9]). Intercept applications are authorised by the Minister for Justice, Equality and Law Reform.

135. Section 12 of the 1993 Act[10] states that the Minister shall ensure that such arrangements as he considers necessary exist to limit to the minimum necessary the disclosure of the fact that an authorisation has been given and the contents of any communication which has been intercepted. This restriction on disclosure coincides with the practice of An Garda Síochána not to use intercept product as evidence in prosecutions. So, although not prohibited by statute, in practice intercept as evidence is not used in Ireland.

136. This practice is long standing and there are no plans at present to change it. *** On balance, it is believed that the long-term net effect of using intercept evidence would be to reduce both the quantity and quality of intelligence gained and, consequently, the quantity and quality of convictions secured.

137. ***

138. Although a number of the concerns given for justifying the practice of not using intercept as evidence in Ireland are not insurmountable, and indeed have been addressed to varying degrees by countries that do use intercept as evidence, we gave serious consideration to the fact that the legal jurisdiction closest to the UK's has decided against the use of intercept as evidence. This comparison underlines the need for the UK to conduct such an analysis ourselves, as we have done in this Report.

Netherlands

139. Intercept in the Netherlands is carried out through two entirely separate systems of intelligence and law enforcement intercept.

140. Law enforcement interception is authorised by the Special Powers of Investigation Act, which came into effect in 2000. It allows for interception in cases of serious crime (four or more years imprisonment), on the authority of an examining magistrate. Interception is carried out by the National Police, under the coordination of the Platform for Interception, Decryption and Signals Analysis. Its capability has significantly improved recently. The value of intercept as evidence is almost always dependent on being combined with other evidence, particularly in organised crime cases. *** All intercept material has to be retained, examined (not necessarily in real time) and noted; relevant material has to be fully transcribed. All material (but not the methods by which it was obtained) has to be disclosed to the defence, at the risk of disclosing capability through knowledge of intercept having taken place. ***

[9] Chief of Staff of the Permanent Defence Forces may also apply for an authorisation in interest of security of the State

[10] The Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993

141. The Dutch security service[11] is authorised to intercept on the personal authority of the Ministry of the Interior. By law, all national security information (including sources and methods of interception) must be kept secret. ***

142. The Netherlands provides a clear illustration of how intercept as evidence can be used extensively and successfully as an integral part of combating serious crime. Their law enforcement practitioners find it hard to conceive of fighting serious organised crime without using intercept material as evidence. ***

Spain

143. In Spain judicially authorised intercept is admissible in cases of serious crime, including terrorism[12].

144. The Supreme Court has established rules for authorising interception and the handling and use of the intercept product. The authorisation relates only to specific telephone numbers in relation to a specific investigation. The whole operation must be under judicial control right through to its conclusion; the original intercept tapes must be submitted in their entirety to the Court, accompanied by typed transcripts of their content. The transcription of conversations is not a legal requirement, but in practice a transcript is handed to the Court as it summarises the content of recordings and is used to locate segments of a conversation.

145. Before the trial, all intercepted material is disclosed to the defence. The prosecution or defence can request conversations to be played during the oral court proceedings in the presence, where appropriate, of the police who conducted the investigation, so that they can explain the techniques used, how the recordings relate to the stages of their investigation, and how they have interpreted the conversations. If the conversations are in a foreign language, an interpreter must be present. Technical tests to verify the identity of the speakers can also be requested.

146. Spanish authorities state that the overall results of using such intercept for criminal investigation and evidence have been very positive. ***

147. ***

148. *** Until recently, intercept conducted by intelligence services was not admissible in court. However, with the establishment of the new National Intelligence Centre (CNI) and subsequent reorganisation of the intelligence services, the intelligence services can now intercept with legal authorisation[13] from a magistrate, in which case the product is admissible in court if other jurisprudential requirements have been met.

[11] AIVD – Algemene Inlichtingen en Veiligheidsdienst
[12] Serious crime - terrorism, drug trafficking, illegal immigration, forgery, and credit card cloning, money laundering and any other organised crime
[13] According to Organic Law 2/2002 of 6 May 2002

149. Spain provides another example of a country that uses intercept as evidence extensively to support criminal prosecutions for serious crime, including terrorism. ***

COMMON LAW COMPARISONS

Australia

150. Australian legislation allows for two kinds of warrant: for law enforcement (granted by a judge or member of the Administrative Appeals Tribunal); and for intelligence (granted by the Attorney General). A warrant can only be granted as a 'last resort' if alternative methods of investigation are not available, and after consideration of the balance between the gravity of the conduct being investigated and the degree of interference with the privacy of the individual.

151. All law enforcement intercept is useable in evidence; indeed, law enforcement interception can be authorised only for this purpose. *** All intercept product is retained until the end of the trial process. Agencies are required to transcribe only the material they intend to make use of in court. Normal practice is to disclose to the defence a compendium of all the intercept; as a matter of practice the prosecution do not attempt to identify exculpatory material. Judges take a robust line in requiring the defence to give reasonable limits to any request to examine the underlying material. The scale and practice of law enforcement use of intercept varies from State to State.

152. To introduce interception into court proceedings, the relevant agency and service provider provide the court with an Evidentiary Certificate[14], which is prima facie evidence for the lawfulness, authenticity and integrity of the intercept. In recent cases, the defence have sought more detail of interception processes, which the State has declined to provide. ***

153. ***

154. The National Security Information (Criminal and Civil Proceedings) Act 2004 provides a means of introducing classified material into a criminal case in sanitised form. The material is shown to the judge and cleared defence counsel – who are forbidden to reveal the material to their clients. *** More commonly sensitive capabilities are protected against disclosure by Public Interest Immunity. ***

155. *** Interception both provided lead evidence and corroborated other evidence (especially from turned accomplices). It often resulted in guilty pleas. The Annual Report of the use of the Telecommunications (Interception and Access) Act 1979, for the year ending 30 June 2006, stated that there were:

[14] In accordance with Section 61 of the Telecommunications (Interception and Access) Act 1979

- 2024 arrests on the basis of lawfully intercepted information;
- 3007 prosecutions (for drug offences, organised crime, murder etc.); and
- 1486 convictions (for the same offences – although none for terrorism[15]).

156. Although these statistics do not precisely indicate to what degree intercept material directly used in evidence was critical in securing these convictions, Australia does appear to us to be a compelling example of how intercept as evidence can be used in a Common Law jurisdiction (but one not within the scope of the ECHR) to combat serious crime[16]. Their approach also provides a number of more detailed ideas for the UK to consider, including:

- The establishment of 'national intercept standards' which reduce the risk of defence challenge of technique;
- Evidentiary Certificates that act as evidence of lawfulness, authenticity and integrity of intercept; and
- Provisions of the National Security Information (Criminal and Civil Proceedings) Act 2004, allowing for closed hearings with cleared defence counsel and summarised disclosure of sensitive evidence, which provide added protection against disclosure that could prejudice national security.

Canada

157. Canada conducts intercept both for law enforcement purposes and for foreign intelligence purposes, with the two forms of intercept kept distinct in law and practice. Interception for law enforcement is authorised by a judge on application from a prosecutor, as long as the minimum requirements have been met that: it is in the best interests of justice to do so (meaning there are reasonable grounds to believe that the specified crime has been or is being committed); and that there are no other reasonable means of investigation.

158. All law enforcement intercept ("wiretap") material is useable in evidence and is subject to disclosure rules. The Crown has an obligation to disclose to an accused all information, whether inculpatory or exculpatory, unless it is clearly irrelevant, beyond the control of the prosecution or subject to a legal privilege. Part VI of the Criminal Code allows the prosecutor to edit the wiretap application documents before they are disclosed to the defence in order to maintain confidential informants and information, which would also be protected under police investigative privilege. The subject of the intercept must be notified of the fact of interception at the time charges are laid. Intercept evidence is frequently the subject of challenges on statutory and '*Charter of Rights and Freedoms'* grounds, as well as on technical grounds such as tape integrity, accuracy and voice identification.

[15] Although there were 10 prosecutions for terrorism offence that used intercept product in that year, there were no convictions.
[16] Our Two Warrant model (see Chapter VIII) draws significantly on the Australian experience.

159. Although over 90% of offences investigated using wiretap as an evidence gathering technique resulted in convictions, the proportion was far lower in those cases where intercepted material was adduced in evidence; between 20% and 46% from 2001-2003[17]. Although part of the difference in these figures may be attributable to differences in statistical gathering techniques by the agencies involved, it also appears to indicate that a significant part of the benefit of the use of intercept in Canada is from its use as an investigative tool, as already used in the UK.

160. However, the Royal Canadian Mounted Police (RCMP) have told us they are convinced of the value of intercept for law enforcement purposes. *** We understand that it is often critical to trials.

161. The Canada Evidence Act (CEA) 1985 provides in section 37 for the protection of police techniques, intelligence and informants in the public interest. Once a court is notified of an objection to disclosing information on section 37 grounds, the court will determine whether the public interest in disclosure outweighs the public interest in non-disclosure.

162. In addition, section 38 provides stronger protection for sensitive national security, national defence or international relations information. Those involved in proceedings where such information may be disclosed must notify the Attorney General. Once this notice is sent, there is a statutory prohibition on the disclosure of the information. The Attorney General must make a determination whether to authorise disclosure or not, after balancing public interests in disclosure or non-disclosure. His decision may be appealed to the Federal Court of Canada.

163. Section 38 of the CEA is an important protection to allow the Canadian intelligence agencies[18] to provide information to law enforcement. Because of the intelligence agencies' own mandate and the increasingly transnational nature of criminal activity, it is felt to be in the national interest that they provide such support. However, it is recognised that there is an increased risk of disclosure arising from their interaction with law enforcement, due to an accused's broad constitutionally protected right of disclosure from the Crown. The intelligence agencies generally rely on RCMP to notify them if any information they have provided may be relevant to a criminal proceeding. They are then able to determine whether to notify the Attorney General that disclosure of the information could injure international relations, national defence of national security, in accordance with section 38.

164. Where the intelligence agencies have been involved in section 38 CEA proceedings, they has been required to provide evidence in support of the claim that disclosure of the information would be injurious. Evidence is provided to the Federal Court by way of an *ex parte* affidavit (i.e. a copy of the affidavit is not provided to counsel for the accused), and oral testimony is heard in closed session, with only the cleared counsel for the Attorney

[17] Annual Report on the use of Electronic Surveillance, 2005
[18] The Communications Security Establishment (CSE), the Canadian equivalent to GCHQ, and the Canadian Secret Intelligence Service (CSIS).

General present, before a judge of the Federal Court designated to hear matters of national security sensitivity.

165. The challenge of using intelligence, including intercept, as evidence is currently being reviewed in Canada by the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 1982.

166. The Canadian approach provides another clear example of how law enforcement agencies make effective use of intercept to help secure convictions of serious criminals. However, much of this benefit appears to be derived from using intercept as an investigative tool, rather than through adducing intercept product directly in court. They have also developed added protections to protect sensitive national security information, which helps to enable intelligence agencies to support law enforcement investigations, although some risk of disclosure remains.

167. As with the Australian system, and the protections provided by their National Security Information Act, the Canadian legal regime, in particular the CEA section 38 proceedings, have provided useful ideas for our consideration of the type of legal regime that could be developed in the UK.

United States

168. The United States has two quite separate systems for authorising the interception of communications: "Title III"[19] is used to authorise interception for law enforcement, while interception for foreign intelligence purposes is authorised by FISA[20]. FISA interception is not permitted unless it is certified that the information sought cannot reasonably be obtained by other means. Title III intercept is routinely used as evidence in criminal cases; FISA intercept is not.

169. Historically FISA intercept was used almost exclusively as foreign intelligence. But since 9/11 cooperation between intelligence and law enforcement has improved, and the product of intelligence interception has been shared between the intelligence and law enforcement communities. ***

170. Law enforcement agencies keep all material at least until the case ends. Only relevant material is transcribed, but defence counsel are beginning to demand indexes to the entire material. Intelligence agencies only keep intercepted material as long as is required for their own purposes. ***

171. US law provides a broad definition of discoverable material. In cases where intelligence material is involved, the discovery process begins with letters to the agencies outlining the case. The prosecution then have to review all relevant material held by the agencies. *** If sensitive material is determined to be discoverable, it is managed under the Classified Information

[19] Title III of the Omnibus Crime Control and Safe Streets Act (Wiretap Act) 1968
[20] FISA – Foreign Intelligence Surveillance Act 1978. This is likely to be replaced by a new Act in 2008, but we understand that the essentials will not change.

Procedures Act 1980 (CIPA). This allows material to be shown to the judge alone, who can rule that

- it need not be shown to the defence;
- it must be disclosed (in original or redacted form) to cleared defence lawyers; or
- It must be disclosed (in original or redacted form) to the defendant.

***

172. CIPA gives the right to appeal any disclosure decision before actual disclosure occurs. In some instances defence counsel can be cleared to review classified material on the client's behalf. So long as the defence can adequately represent their client without classified information, the court can forbid discussion of sensitive matters with the client. *** In particular the proceedings of the Foreign Intelligence Surveillance Court, which authorises interception under FISA, have never been revealed to the defence.

173. New technology presents a challenge for both intelligence and law enforcement. *** As stated in Chapter VI, we do not expect the US to use the product of its most sensitive new techniques in evidence.

174. US law enforcement see intercept as evidence as an invaluable tool. They generally use intercept in conjunction with other evidence, but playing a tape in court can be critical. Intercept can corroborate informant and documentary evidence, and (used in conjunction with plea bargaining) frequently results in guilty pleas and willingness to cooperate. When this happens, cooperating defendants can help explain the meaning of intercepted material to the court, so securing the conviction of top-level criminals. Most large organised crime cases include intercept evidence, as do many white-collar crime cases. Intercept product was a critical part of a series of operations that resulted in the conviction of the five major New York mafia bosses.

175. The United States experience illustrates how intercept as evidence can be used to combat serious crime. However, in *** cases where the most sensitive intercept techniques are used, their product is seldom used as evidence, because of the risks of capability being compromised.

176. In making comparisons between the US and UK systems, it is important to recognise that UK law enforcement and intelligence agencies currently use intercept to combat serious crime and terrorism at least as extensively as the US, using intercept as a criminal intelligence and investigative tool, despite the US population being five times greater. ***

177. The resulting UK conviction rates are also relatively impressive. In the US, even allowing for a time lag between the date of interception and eventual arrest and conviction, the highest arrest to conviction rate, as a result of interception, between 1996 and 2006 was 56.4%[21]. In the UK, a Metropolitan police study of operations carried out involving intercept as intelligence only in

[21] Administrative Office of the United States Courts 2006 Wiretap Report

2006-2007, found that there was an 88% charge to conviction rate of completed cases[22]. This conviction rate is consistent with the 85% arrest to conviction rate of HMCE drugs operations supported by intercept in 2001/02, as reported in the 2003-04 Multi-Agency Review of Intercept as Evidence.

RELEVANCE OF COMPARISONS TO UK

178. In all of the examples examined, other than the Republic of Ireland, the respective law enforcement agencies and prosecuting authorities asserted strongly that intercept as evidence was a valuable tool to enable them to combat and convict serious criminals. The value of intercept product as evidence to secure terrorism-related convictions was generally less clear. There was also no conclusive proof that other countries' use of intercept as evidence resulted in higher conviction rates for serious crime than the UK's approach of using intercept as an investigative and criminal intelligence tool.

179. The ways in which each country had developed their evidential regimes, and managed the risks and costs, varied considerably and were shaped by their respective criminal justice systems.

180. We believe that the approaches adopted by the EU countries, other than the Republic of Ireland, tend not to have great relevance for the UK, for a number of reasons:

- The examining magistrate system of criminal proceedings combines investigative and judicial functions within one role, with the examining magistrate able to authorise intercepts to develop the investigation for which he/she is responsible. Once the case comes to trial, defence questioning of this case is far less rigorous than under the UK system. This means that the risks of disclosure of sensitive techniques or content is considerably lower than it would be in the UK, whilst at the same time being less open to ECHR Article 6 challenge, as the intercept has been produced as part of a judicially overseen enquiry.
- In France, The Netherlands and Spain, law enforcement agencies' efforts to combat serious organised crime and terrorism receive less support from their security and intelligence agencies than is the case in the UK. We have concluded that the price of adopting such a clearly split system of intercept in the UK would be a significant reduction in the amount of day to day support provided to serious crime investigations in the UK by the intelligence services' intercept capabilities.
- ***

181. The Common Law examples are of greater relevance. They illustrate how intercept as evidence has been introduced into adversarial criminal justice systems, with a number of approaches adopted to protect against disclosure of sensitive capabilities and techniques.

[22] Of 218 individuals: 104 convictions so far; 7 acquittals; 13 not proceeded with; 94 still awaiting trial

182. However, even with these examples we have found some important differences that need to be considered:

- The interwoven nature of the current use of intercept by UK law enforcement and intelligence agencies, to combat serious crime and terrorism, and the cooperation and support they provide to each other does not exist to the same degree in Australia, Canada or the United States.
- These countries are not bound by ECHR. Such aspects of their systems (such as transcribing only that material which the law enforcement agencies intend to use in court, and using closed hearings in criminal proceedings) would need to be judged ECHR Article 6 compliant if they were to be replicated in any UK system.
- US prosecutors are able to use intercept material together with plea-bargaining, to "turn" defendants and to secure early guilty pleas. This experience might not be replicated in the UK, where plea-bargaining in the US sense is not permitted.

183. The Common Law countries examined by this Review have tended to adopt a dual warrant approach, separating intelligence and law enforcement use of intercept. The Australian example, in particular, provides a number of interesting ideas for how the UK could attempt to derive benefit from intercept as evidence, whilst not unacceptably increasing the risk of disclosure to intelligence agencies and their sensitive capabilities and techniques, and allowing for cooperation between intelligence and law enforcement agencies to continue.

184. The 'Two Warrant Model' which we have developed, and which is set out in greater detail below in Chapter VIII, has been informed by the Australian approach.

CHAPTER VIII - LEGAL MODELS

INTRODUCTION

185. The present legal model for interception (see Chapter II) precludes the use of intercept as evidence in any ordinary legal proceedings. If this is to be changed, there are a number of legal issues, following from the European Convention on Human Rights (ECHR), that must be taken into account in devising a new model. In addition to being legally sound any new model has, of course, to be operationally practicable, affordable and effective.

186. Several such models have been considered in previous Government reviews of Intercept as Evidence, or have been proposed by interested parties outside Government. The present Review has re-examined all of these. We decided to look in some detail at three candidate models:

- The "PII Plus" model developed late 2006 – early 2007;
- A model developed for this Review by Lord Carlile of Berriew QC; and
- A new "Two Warrant" model developed by the Review, based in particular on the system used successfully in Australia, and elaborated to take account of the needs of interception in the IP era.

These are covered in separate sections below. We have carefully considered other models that have been put forward in the past, but conclude that none of them are viable options.

187. The Review has sought Counsel's advice from Jonathan Crow QC on the three candidate models. We asked for his opinion on

- Whether the three candidate models complied with the European Convention on Human Rights (ECHR);
- If not, whether they could be modified to do so, without putting sensitive capabilities at risk or imposing unreasonable burdens on the intercepting agencies;
- If a new model was adopted and failed, whether it would then be legally possible to revert to the *status quo*.

LEGAL ISSUES

188. Two Articles of the ECHR are principally engaged when considering the use of Intercept as Evidence. These are

- Article 6, which guarantees the right to a fair trial, and
- Article 8, which deals with the right to private and family life.

189. A number of relevant principles have been derived from Article 6. They include

- There must be fair disclosure of the case to the defence. In English law[23] this is regulated by the Criminal Procedure and Investigations Act 1996 (CPIA), which imposes a duty on the prosecution to retain all material that might be relevant, and to disclose
    - all material on which the prosecution relies, and

[23] In Scotland a different system applies – there is no equivalent to PII.

    - any 'exculpatory material' - unused material that materially supports the defence case or materially undermines the prosecution case.

  The right to disclosure of exculpatory material is however not absolute. The House of Lords has ruled[24] that exculpatory material can be withheld by virtue of Public Interest Immunity (PII) if
    - there is an important countervailing public interest,
    - non-disclosure is strictly necessary to protect this interest, and
    - any difficulty caused to the defence can be sufficiently counterbalanced to ensure a fair trial.
- The State must not be able to 'cherry pick' material so as to give itself an unjust advantage over the defendant. This could for example happen if investigators can choose to intercept evidentially only those lines they believe will yield incriminating material, while protecting other product from disclosure that contained exculpatory material. If cherry picking was suspected, the defence could apply to the judge to stop the trial on abuse of process grounds. The concept of cherry picking does not of course preclude investigators from making reasonable decisions; they have to decide to pursue some offences and not others, and to use some techniques and not others, for proper reasons of deploying their limited resources to best effect.
- There must be equality of arms between the prosecution and the defence. A defendant must have the opportunity to present his case under conditions that do not place him at a substantial disadvantage. This principle may impose requirements that intercepted material not be deliberately destroyed before a trial, and that its content be noted to a sufficient standard to allow the defence to prepare a case adequately. The European Court of Human Rights (ECtHR) has ruled[25] that current UK interception law is consistent with this principle, as neither the prosecution nor the defence can make use of intercept in court.

190. Article 8 relates mainly to the circumstances in which interception (which is always a serious invasion of privacy) can be authorised, and in which the product can be retained or disclosed to third parties. However the ECtHR has ruled in this context[26] that the entirety of any potentially admissible product must be retained and disclosed to the defence. The Government has been advised that this ruling does not apply to the UK's current situation. We have heard very different views on its relevance to the UK if intercept was used as evidence. We were told by both the French and the Dutch that they did not believe the ruling applied to their situations, which are closer to the Spanish than any model being considered for the UK. This view has yet to be tested before the courts.

[24] *R v H and C* [2004] UKHL 3
[25] *Jasper v UK* (2000) 30 EHRR 441
[26] *Valenzuela Contreras v Spain* (1998) 28 EHRR 483

CANDIDATE MODELS

PII Plus

191. All intercepted material would be potentially admissible as evidence. Agencies could decide whether or not to conduct interception to evidential standards (there would not be different kinds of warrant). If they chose to conduct interception evidentially, they would record and retain all the product. They would be required to transcribe any sections required by the prosecution, and to keep minimal records of the rest. If they did not so choose, they would handle the material as required for intelligence purposes, and additionally retain for later review any material judged to be exculpatory. Standards for retention and recording would be set out in statutory guidance, which would exist in both public and classified versions.

192. Once charges had been laid, all potentially exculpatory material would be reviewed along with other unused material; if it met the threshold for disclosure, it would be disclosed to the defence subject to Public Interest Immunity (PII). Closed hearings, at which the defendant's interest would be represented by a Special Advocate, would be used to address any defence challenges to the admissibility of intercepted material where sensitive technical information was relevant.

193. PII would be enhanced and put on a statutory basis, replacing the current case law that has evolved over several years. The statute would set out the process to be followed in deciding what material is liable to be disclosed to the defence, and what the prosecution and the trial judge must do if there appears to be a public interest against disclosing certain information. There would be a right of appeal for both sides against the trial judge's decision, and a statutory bar on judges ordering the disclosure of sensitive material. Instead the judge would have to stop the trial if he concluded that a fair trial was not possible. While the question is outside this Review's scope, we suggest that any new statutory PII should apply to all sensitive material, not just intercept.

Lord Carlile's Model

194. Intercepted material would be potentially admissible as evidence, provided that the admission of the evidence is necessary in the interests of justice in the specific case. If this criterion is met it would be for the prosecution to decide whether to use intercept evidence in a case.

195. If current guidelines required exculpatory intercept to be disclosed, and the Attorney General certified that disclosure would be adverse to the national interest, a special regime would apply. A closed *ex parte* hearing would be held before a judge appointed by the Master of the Rolls[27] (with a Special Advocate to represent the defendant's interest if the judge so requires) to

[27] Alternatively the trial judge could be appointed in this way, and deal with disclosure as well as running the trial.

decide whether disclosure was needed, and if so whether it could be made (for example in a redacted form or as an admission of fact) in a way that protected the relevant sensitivity. In the absence of such a certificate normal disclosure rules, with PII available if relevant, would apply.

196. Standards for retention and recording of intercepted material would be set out in statutory guidance.

Two Warrant Model[28]

197. Warrants attracting the current RIPA s17 protection would still be available, but only to the intelligence agencies. The product of such warrants would not be admissible as evidence; before a trial the prosecution would still have a duty to review any relevant intercepted material obtained by the intelligence agencies, in order to determine what is required to secure the fairness of the trial (see Chapter II). The intelligence agencies would be able to accept tasking from law enforcement and provide reports based on interception – the reports (rather than the original material) would form the basis of the prosecution's review. There would be a statutory ban on the revelation of intelligence capabilities and techniques in court.

198. A new parallel regime would be set up, by which warrants for interception by agencies other than intelligence agencies would be given by selected judges. The resulting material would be handled in accordance with CPIA rules; it would be admissible as evidence, and discloseable subject to current guidelines. Any defence challenges to the legality or integrity of the intercept will be dealt with *ex parte*, with a Special Advocate representing the interests of the defendant. PII, put on a statutory basis (see previous section), would be available if required.

199. Protection of the sensitive capabilities involved in interception in the IP era (see Chapter VI) could be enhanced by making the product of defined techniques inadmissible as evidence. Enhanced protection from disclosure of any exculpatory material of this kind would also be required. PII would be unlikely to provide the required protection, as the sensitivity would lie in the capability to intercept communications of certain kinds (not just the techniques used to achieve this), which could only be protected by withholding the whole of the product.

VIABILITY OF CANDIDATE MODELS

200. The independent legal advice provided to the Review by Jonathan Crow QC suggests that there might be substantial legal difficulties with using intercepted material as evidence in the UK's situation, regardless of which legal model is chosen. These difficulties include:

- The courts might show antipathy to the routine destruction of intercept on which the authorities did not intend to rely, and which they had not identified as exculpatory. If relevant material was not recorded and

[28] So called for the sake of distinction from an earlier Dual Warrant model.

preserved in its entirety, there would be an increased risk that the regime would be held not to produce a fair trial.
- There would be an enhanced risk of successful challenges being brought by the defence if all product was not required to be noted, indexed and preserved to a high standard. If relevant material was simply recorded, without being monitored, noted and indexed, there is an increased risk that the regime would be held not to produce a fair trial.
- If the defence was deprived of any effective opportunity to challenge the authenticity and accuracy of any material, it would undermine the prospect of successfully defending the ECHR compatibility of the regime.

201. There are also features of any regime that might mitigate these difficulties and contribute to the regime's compatibility with the ECHR. These include:
- Express statutory enactment. In order to satisfy the ECHR test of legality it would be highly desirable for as many features of the regime as possible to be set out in primary legislation. Notwithstanding that general advice, he advises that there would be no clear benefits in seeking to codify the PII regime in statute (others have taken a different view).
- Judicial supervision. One of the fundamental concerns underlying the ECHR is to prevent the arbitrary exercise of executive power over the individual. As such the ECtHR is always comforted if the exercise of any executive power is tempered by judicial supervision.
- Special advocates. It would further assist in providing an effective form of judicial supervision if special advocates were available when necessary in order to introduce an adversarial element into the process.
- Supervision by the Interception Commissioner.

202. Turning to the specifics of the candidate models, the advice is that:
- There is no fundamental flaw in the ECHR compatibility of the PII Plus model;
- Lord Carlile's model represents a variant of the PII Plus model; it equally has no fundamental flaw, but offers no advantages over PII Plus;
- The Two Warrant model contains a fundamental flaw that would expose it to a significant risk of successful legal challenge, in that it would afford different treatment to intercepted material based only on the agency which intercepted it, failing to meet the requirement that any measure that restricts the rights of the defence must be shown to be strictly necessary. This flaw cannot be rectified by any small change to the model.

203. If a new model were to be adopted and then fail for any reason, the advice is that it would be legally possible, in terms of ECHR compliance, to revert to the current situation with intercept barred from most legal proceedings. We were advised that the fact of an attempt to use intercept in

evidence, and the failure of that attempt, would add weight to a contention that a bar on intercept as evidence was an appropriate balance between the legitimate needs of the State and the rights of individuals.

CHAPTER IX – CONCLUSIONS AND RECOMMENDATIONS

204. The State has an overriding duty to protect the public, including from threats such as international terrorism and serious organised crime. One important contribution to this duty is to prosecute cases of serious organised crime and terrorism whenever possible. This requires that the best evidence is made available for such prosecutions. At the same time the trials must be (and be seen to be) fair. The Review is confident that these two objectives would be supported by the use of intercept as evidence. **We therefore agree with the principle that intercept as evidence should be introduced.**

205. However, the ability to prosecute serious organised crime and terrorism is only one way of achieving the protection of the public. We would therefore support intercept as evidence only if, on balance, it would at one and the same time safeguard national security, facilitate bringing cases to trial and allow the effective use as intercept as intelligence to continue.

206. We believe a legal regime could be devised that should be ECHR compatible. No such regime has yet been fully developed, but we believe one could be along the lines of the PII Plus model described in Chapter VIII. It would make all intercepted material, whether originating in intelligence or law enforcement agencies, potentially useable as evidence, **without of course compelling such use**. Sensitive capabilities would need to be protected by PII.

207. Any legal regime must address the following costs and risks:

- The potential need for intelligence as well as law enforcement agencies to preserve and perhaps monitor an enormous amount of intercept product which might be relevant to future criminal cases.
- A risk of disclosure of intercept capabilities and techniques, including those of the intelligence agencies. We understand and accept that no absolute guarantee can be given, but none of the legal models looked at up to this point have by themselves provided in our view a sufficient basis to strike the right balance between ensuring a fair trial, including defence ability to probe the integrity of intercept product, whilst ensuring that disclosure of intercept capabilities and techniques is kept to an acceptable level. The heightened risk of disclosure is a direct result of lifting the ban on prosecution use of intercept product and the need to ensure that a new ‘equality of arms’ balance is struck. This risk is inherent in any realistic legal model, and will have to be addressed by separate Government undertakings to abandon cases if necessary to prevent damaging disclosure.

208. Although we believe that a legal regime could be developed that is ECHR compatible and enhances justice by enabling intercept evidence to be adduced in court, any such regime would also need to meet the following operational requirements as set out in Chapter IV, in order to ensure that the UK’s strategic intelligence capability was safeguarded and the ability of intelligence and law enforcement agencies to protect the public was not harmed:

- The intercepting agency shall decide whether a prosecution involving their intercepted material shall proceed.
- Intercepted material originating from the intelligence agencies shall not be disclosed beyond cleared judges, prosecutors, or special (defence) advocates, except in a form agreed by the originator.
- Material intercepted (by any agency) through the use of sensitive Sigint techniques shall not be disclosed unless the Secretary of State is satisfied that disclosure will not put the capability and techniques at risk.
- No intelligence or law enforcement agency shall be required to retain raw intercepted material for significantly more or less time than needed for operational purposes (which may include using the material as evidence).
- No intelligence or law enforcement agency shall be required to examine, transcribe or make notes of intercepted material to a higher standard than it believes is required to meet its objectives (which may include, but are not limited to, using the material as evidence).
- Intelligence and law enforcement agencies shall be able to carry out real time tactical interception in order to disrupt, interdict or prevent terrorist and criminal activity, as effectively as they do now.
- Law enforcement agencies shall be able to use interception to provide strategic intelligence on criminal enterprises, and retain the intelligence sometimes for a number of years, regardless of the progress of specific criminal cases. Interception from the same lines may meet both tactical and strategic purposes; if it does, it shall be handled in a manner appropriate to both.
- Intelligence agencies must be able to support law enforcement by carrying out interception, for 'serious crime' purposes, of targets nominated by law enforcement, and to provide the product or reports on it to those agencies. Anything so provided shall be subject to the same disclosure obligations as other intelligence intercept.
- At trials (whether or not intercept is adduced as evidence) the defence shall not be able to conduct successful 'fishing expeditions' against intercept alleged to be held by any agency.

209. The benefits of the current use of intercept as an investigative tool are largely due to a number of specific characteristics in the way that the UK law enforcement and intelligence agencies are organised and co-operate:

- There is uniquely close and valuable cooperation between UK intelligence and law enforcement agencies.
- Law enforcement agencies (primarily SOCA) use intercept to gather complex intelligence pictures sometimes over many years, whilst in other instances they use intercept to move swiftly, particularly when life is at risk.
- GCHQ and Security Service provide extensive operational and (critically) technical support to law enforcement operations.
- The UK has a particularly large and sophisticated intercept capability, which is used flexibly and efficiently.

210. We believe that a limited number of new successful prosecutions would be made possible by the use of intercept as evidence. The UK already achieves very high rates of successful prosecution of serious criminals and terrorists; there is limited room for substantial further improvement in such cases through the use of intercept as evidence. We have not seen any evidence (see Chapter III) that the introduction of intercept as evidence would enable prosecutions in cases currently dealt with through Control Orders.

211. We need so far as possible to enable the UK to retain the immense value to public protection of the current use of intercept as an investigative tool together with close intelligence agency and law enforcement cooperation whilst improving justice by removing the ban on intercept as evidence with marginal costs to the current arrangements.

212. We recognise that there are substantial fears among those who operate the present system that any model for intercept as evidence, however robustly constructed, might later encounter legal difficulties which could damage the essential national security interests described above. They rightly believe that these interests must be protected.

213. In order to develop the necessary confidence **we recommend that, if the Government decides to introduce an intercept as evidence regime, it provides an undertaking at the outset that it would take action if either the practical operation of the regime or subsequent adverse legal rulings meant that the operational requirements set out above could no longer be met**. An adverse legal ruling should involve no loss of security: a criminal court cannot oblige the Government to release sensitive material, as the Government always has – and must be prepared to exercise – the option of abandoning the particular prosecution. In the event of adverse rulings action would consist either of modifying the new regime to meet the particular difficulty, or of returning to the current regime. **The Government would in this way make clear that in no circumstances would there be a sacrifice of the essential security requirements we have listed.**

214. Before legislation could be introduced along these lines, further extensive work would be required to develop a detailed regime by:

- completing the development of an ECHR compatible legal model, based in statute, starting from the PII Plus model;
- exploring the operational consequences of such a model and devising pragmatic ways to reconcile divergent interests;
- in advance of any repeal of RIPA s17, ensuring that such a regime met the operational requirements set out above; and
- creating confidence amongst the relevant interests (including communication service providers and international partners) that the introduction of such a regime would enhance justice and public protection in the UK, whilst safeguarding national security and partners' legitimate needs.

215. For the reasons set out in detail in Chapter IV, we recommend that for the time being no change to the current legal regime for interception be

considered for cases in the civil courts, in Scotland (at any rate before new disclosure legislation is in place), or in Northern Ireland.

216. **We conclude that it would be possible to provide for the use of intercept as evidence in criminal trials in England and Wales by developing a robust legal model, based in statute and compatible with ECHR, starting from the PII Plus model described in Chapter VIII. We recommend that the Government, in order to achieve this, put in hand the confidence-building measures and the work set out above.**

ANNEX A – WAY OF WORKING

We have carried forward this Review on Privy Council terms throughout. We have therefore invited all interested parties to meet us and/or to provide written submissions at whatever level of sensitivity they deem appropriate. The meetings we had and the submissions we received are listed at Annexes B and C respectively. We visited France and the Netherlands for discussions, and had videoconferences with representatives of the Australian and US governments.

We have had access to all the previous studies carried out within Government, and in particular to the extensive legal advice that supported them. We additionally sought Counsel's advice ourselves, independently of that previously provided to Government.

We agreed not to publish the representations and submissions made to us. They have of course been the major influence on this Report and on the conclusions it reaches. Where we believe it helpful we have drawn material for this Report from the evidence offered to us, with the originators' agreement. The conclusions of the Report are by contrast those of the Review Members alone, and have not been cleared in advance with anyone outside the Review.

We are grateful to all those who agreed to meet us, or to provide input in writing, for the efforts they had without exception taken to inform us of the issues, and for providing us with their frank views. Without this help we would not have been able to carry out this Review.

The overall cost of the Review has been £115000.

ANNEX B – LIST OF WITNESSES

Attorney General's Office

Government of Australia

Judge Barker

British Telecommunications plc

Cabinet Office

Lord Carlile of Berriew QC

Crown Prosecution Service

Andrew Dismore MP

Foreign and Commonwealth Office

Government of France

Lord Goldsmith

Government Communications Headquarters

Her Majesty's Revenue & Customs

Home Office

Rt Hon Michael Howard QC MP

Interception of Communications Commissioner (Sir Paul Kennedy)

Sir Igor Judge

JUSTICE

Sir Brian Leveson

Lord Lloyd of Berwick

Liberty

Lord Chief Justice

Michael Mansfield QC

Metropolitan Police

Government of the Netherlands

Northern Ireland Office

Baroness Park of Monmouth

Police Service of Northern Ireland

Baroness Ramsay of Cartvale

Judge Roberts

Royal Mail

Secretary of State for Justice

Security Service

Serious and Organised Crime Agency

Strathclyde Police

Nigel Sweeney QC

Treasury Solicitor

Embassy of the United States of America

Stephen Williamson QC

ANNEX C – LIST OF WRITTEN SUBMISSIONS

Association of Chief Police Officers

Association of Chief Police Officers for Scotland

British Telecommunications plc

Cabinet Secretary for Justice (Scotland)

Crown Prosecution Service

Lord Goldsmith

Government Communications Headquarters

Her Majesty's Revenue & Customs

Rt Hon Michael Howard QC MP

Intelligence and Security Committee

Internet Service Providers Association

JUSTICE

Sir Paul Kennedy

Lord Lloyd of Berwick

Lord Advocate

Metropolitan Police

Ministry of Defence

Northern Ireland Public Prosecution Service

Office of Criminal Justice Reform

Police Ombudsman for Northern Ireland

Police Service of Northern Ireland

Simon Price

Royal Mail

Secret Intelligence Service

Security Service

Serious and Organised Crime Agency

Serious Fraud Office

Professor John Spencer QC

Vodafone plc

And from the governments of the following countries:

Australia

Canada

Germany

Republic of Ireland

New Zealand

Spain

Sweden

ANNEX D – BIBLIOGRAPHY

Regulation of Investigatory Powers Act 2000 (Chapter 23)

Interception of Communications: Code of Practice (TSO, 2002)

Anti-Terrorism, Crime and Security Act 2001 Review: Report (the Newton Report) (HC100, 18 December 2003)

JUSTICE *Intercept Evidence: Lifting the Ban* (October 2006)

Report of the Interception of Communications Commissioner for 2005-2006 (HC 315, 19 February 2007)

Evidence for Change – Lifting the ban on intercept evidence in court (Democratic Audit, March 2007)

Lord Lloyd of Berwick *Speech 16 March 2007 introducing the Interception of Communications (Admissibility of Evidence) Bill* (HL Debates Vol 690 Part 60)

Joint Committee on Human Rights *Counter-Terrorism Policy and Human Rights: 28 days, intercept and post-charge questioning* (HL Paper 157 / HC 394, 16 July 2007)

Counter-Terrorism Policy and Human Rights: 28 days, intercept and post-charge questioning (Cm 7215, September 2007)

JUSTICE *From Arrest to Charge in 48 Hours: Complex terrorism cases in the US since 9/11* (November 2007)

ANNEX E - GLOSSARY OF TERMS

Note: all Acts, agencies etc are relevant to the UK unless otherwise stated.

ACPO
Association of Chief Police Officers (for England, Wales and Northern Ireland).

Administrative Appeals Tribunal
An Australian court which can authorise interception for law enforcement purposes.

Anti-terrorism, Crime and Security Act 2001
Part 4 of this Act allows for the detention of foreign nationals suspected of involvement in terrorism, on the basis of closed evidence. These powers have been superseded by those for Control Orders (see below).

Appeals Commission
See Proscribed Organisations Appeal Commission and Special Immigration Appeals Commission below.

CEA
Canada Evidence Act 1985 - sections 37-38 provide for the protection of sensitive material in court.

'Cherry Picking'
Improper action by the State in selecting some of the potentially available material to use evidentially, so as to give itself an unjust advantage over the defendant.

Common Law
The common legal tradition which underlies the laws of the UK, the US and Commonwealth countries such as Australia and Canada.

Control Order
An order made under the Prevention of Terrorism Act 2005 which imposes restrictions on individuals suspected of involvement in terrorism.

CIPA
Classified Information Procedures Act 1980 – a US Act which provides for the management of sensitive material in court.

CPIA
Criminal Procedure and Investigations Act 1996, which regulates the retention and disclosure of potentially evidential material.

CPS
Crown Prosecution Service

CSP
Communications Service Provider – any company that provides communications services to the public or any section of the public.

CT
Counter Terrorism.

Disclosure
The obligatory provision to the defence in a criminal case of relevant exculpatory material (see below) held by the police or other investigating agency, as set out in CPIA (see above). See also Retention below.

ECHR
European Convention on Human Rights, incorporated into UK law by the Human Rights Act 1998. Particularly relevant in the context of the review are: Article 6 (Right to a Fair Trial) and Article 8 (Right to Respect for Private and Family Life).

ECtHR
European Court of Human Rights: the court, based in Strasbourg, responsible for interpreting and enforcing the ECHR. It is an institution of the Council of Europe.

Encryption
A way of protecting a communication by applying a code, the key for which is available only to a limited number of people.

'Equality of Arms'
The principle that, to ensure a fair trial, the same methods and resources should, as far as possible, be available to the defence as to the prosecution.

EU Mutual Legal Assistance Convention
The Convention on Mutual Assistance in Criminal Matters adopted by the EU Council of Ministers in May 2000. It aims to improve cooperation between judicial, police and customs authorities in different EU Member States, and covers cooperation in intercepting communications.

Exculpatory Material
Material held by the police or other investigating agency, which is not intended to be adduced as evidence but supports the defence case or undermines the prosecution case.

FISA
Foreign Intelligence Surveillance Act 1978 – the US Act which regulates interception for foreign intelligence purposes.

GCHQ
Government Communications Headquarters, the UK intelligence agency responsible for communications intelligence and information security.

HMCE
Her Majesty's Customs & Excise – now absorbed into HMRC.

HMRC
Her Majesty's Revenue & Customs.

Inculpatory Material
Material held by the police or other investigating agency which tends to demonstrate the guilt of the accused (whether or not it is intended to be adduced as evidence).

Intercepting Agencies
The UK agencies that can apply for interception warrants are set out in RIPA (see below). The intelligence agencies that may apply are Security Service, GCHQ, Secret Intelligence Service and Defence Intelligence Staff. The law enforcement agencies are HM Revenue & Customs, Serious Organised Crime Agency, Metropolitan Police, Police Service of Northern Ireland and (in effect, for Scotland) Strathclyde Police.

Interception Commissioner
A senior judge appointed by the Prime Minister to oversee the interception provisions in RIPA (see below). The current incumbent is Sir Paul Kennedy.

Interception of Communications
Listening to and/or recording of communications such as phone calls or e-mails as they are being transmitted.

Interception Modernisation Programme
A Home Office Programme which aims to maintain lawful interception in the UK in the face of the move of telecommunications networks to IP technology.

Intercept Product
Anything produced from intercepted communications, including recordings, transcripts, notes and reports.

Intercept Warrant
A formal authorisation from the Secretary of State or the Scottish Ministers in accordance with RIPA, which allows the interception of specified communications.

Internet Protocol (IP)
An international standard method of carrying communications of all kinds (voice, data, internet access etc) in a single data stream.

Investigatory Powers Tribunal
The Tribunal set up by RIPA which considers complaints from the public about interception and other investigatory techniques, and can order appropriate remedies.

Lawful Interception
The interception of communications (electronic or by mail) within the UK in accordance with appropriate legal authorisation (currently RIPA – see below).

Level 1, 2, 3 Criminals
The common definitions are:

- Level 1 – Local level/Basic Command Unit (BCU): crimes, criminals and problems affecting a BCU or small force area. The scope of the crimes will be wide-ranging from anti-social behaviour through to murder. Volume crime will be a particular issue.
- Level 2 – Force and/or regional level: criminal or other specific problems affecting more than one BCU which could cut across other police forces. Issues will be capable of being resolved by forces, perhaps with support from the National Crime Squad, HM Revenue & Customs or other national resources.
- Level 3 – Serious and organised crime: crime that usually operates on a national and international scale. Will usually require help from dedicated units and targeted operations with enforcement and preventative responses on a national basis.

Monitors' Notes
Notes of the significant contents of intercepted communications, which might be used to provide an index to key material. The noting requirement would vary depending on the type of warrant and whether the material was relevant to proceedings.

National Security Information (Criminal and Civil Proceedings) Act 2004
An Australian Act which provides a means of introducing classified material into a criminal case in sanitised form.

NSA
National Security Agency – the US Sigint agency.

NTAC
National Technical Assistance Centre - a part of GCHQ providing specialist technical support to the law enforcement and intelligence agencies. It processes lawfully acquired intercepted communications and stored computer data from the communications service provider to the intercepting agency.

PACE
Police and Criminal Evidence Act 1994.

PII
Public Interest Immunity – see below.

PII Plus
A legal model allowing the evidential use of intercept, developed within Government in 2006-07.

Platform for Interception, Decryption and Signals Analysis
A system used for lawful interception in the Netherlands.

Proscribed Organisations Appeals Commission (POAC)
A tribunal set up by the Terrorism Act 2000 to hear appeals from the Home Secretary's refusal to de-proscribe organisations believed to be involved in terrorism. It can hear closed evidence (including intercept) in private, with the appellant represented by a Special Advocate.

Public Interest Immunity (PII)
A concept of English law whereby material that passes the CPIA test for disclosure can still be withheld from the defence if the judge considers that public interest in withholding it outweighs the public interest in its disclosure. The leading case on PII is *R v H and C* [2004] UKHL 3.

RCMP
Royal Canadian Mounted Police.

Retention
CPIA (see above) sets out procedures handling evidential material gathered during the course of an investigation. It provides that all potentially evidential material gathered during the course of an investigation must be retained and recorded, and that the prosecution has a continuing obligation to review available material and – unless it is sensitive – make relevant material available to the defence. See also Disclosure above.

RIPA
Regulation of Investigatory Powers Act 2000. Part 1 Chapter 1 of this Act regulates the interception of communications; section 17 currently prohibits the use of intercepted communications in criminal proceddings.

s17 Prohibition
Section 17 of RIPA (see above) currently prohibits the use of intercepted communications in criminal proceedings.

SFO
Serious Fraud Office.

Sigint
Short for Signals Intelligence. Interception of electronic signals of all varieties, usually of foreign origin, and the production of intelligence based on that intercept.

SIAC
Special Immigration Appeals Commission (see below).

SIS
Secret Intelligence Service.

SOCA
Serious Organised Crime Agency.

SMS
Short Messaging Service – the ability to send and receive text messages to and from mobile telephones.

Special Advocate
A cleared advocate provided to represent the interests of the defence in proceedings at which the defendant and his normal representatives cannot, for security reasons, be allowed to be present.

Special Immigration Appeals Commission (SIAC)
A tribunal set up by the Special Immigration Appeals Commission Act 1998 to hear appeals from immigration decisions based on national security or political grounds. It can hear closed evidence (including intercept) in private, with the appellant represented by a Special Advocate.

Stored Communications
Communications that have yet to begin their transit across the telecommunications network, or have finished it. For example e-mails stored on computer hard drives, answer-phone messages or voicemail on CSP servers. Access to this material does not need an interception warrant; it can be retrieved using a number of police powers such as a production order obtained from a circuit judge under PACE. In these situations, the s17 RIPA prohibition on evidential use of the material does not apply.

Strategic Intelligence Capability
The national capability to provide intelligence relating to long-term threats to the national security or economic well-being.

'Telecoms Bubble'
The period of the late 1990s marked by the rapid speculative increase in value of telecommunications shares, and the launching of many new Internet companies.

Title III
Title III of the Omnibus Crime Control and Safe Streets Act (Wiretap Act) 1968 provides authority for law enforcement interception in the USA.

Transcript
A verbatim written record of an intercepted conversation (compare with Monitor's Notes, see above).

Voice Identification Techniques
Techniques that aim to identify a speaker (or confirm such an identification) based on recordings of the speaker's voice.

VoIP
Voice over Internet Protocol. The standard means of carrying voice communications over an Internet Protocol network. The voice is 'packetised' (broken up into a large number of separate data messages) to travel across a multiplicity of routes and are only reassembled at the other end.

Warranted Interception
Under RIPA (see above), unless both parties consent or other, specific sections of the Act apply, interception must be authorised by warrant from the Secretary of State or Scottish Ministers. At present, all interception warrants are intelligence-only warrants.

Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office
ID5738265 02/08

Printed on Paper containing 75% recycled fibre content minimum.

Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, Telephone Fax & E-Mail
TSO
PO Box 29, Norwich, NR3 1GN
Telephone orders/General enquiries 0870 600 5522
Order through the Parliamentary Hotline Lo-Call 0845 7 023474
Fax orders: 0870 600 5533
E-mail: customer.services@tso.co.uk
Textphone: 0870 240 3701

TSO Shops
16 Arthur Street, Belfast BT1 4GD
028 9023 8451 Fax 028 9023 5401
71 Lothian Road, Edinburgh EH3 9AZ
0870 606 5566 Fax 0870 606 5588

The Parliamentary Bookshop
12 Bridge Street, Parliament Square,
London SW1A 2JX

TSO@Blackwell and other Accredited Agents

ISBN 978-0-10-173242-0