HM Government

Intercept as Evidence

December 2014

Cm 8989

Intercept as Evidence

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

December 2014

Cm 8989

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at InterceptAsEvidence@homeoffice.gsi.gov.uk

Print ISBN 9781474113410
Web ISBN 9781474113427

ID 12121401 12/14 45598 19585

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office

CONTENTS

EXECUTIVE SUMMARY

1. Interception of communications is one of the most important techniques used in the investigation of terrorism and serious and organised crime. But interception is an intrusive power and is therefore only used by a small number of UK security and law enforcement agencies for a specified range of purposes. While interception supports criminal investigations by providing vital intelligence, the law currently prohibits the use of intercept material as evidence in criminal proceedings.

2. Evidence from overseas jurisdictions, particularly the USA and Australia, suggests that intercept material can be valuable evidence at trial. The Coalition agreement therefore set out an intention to find 'a practical way to allow the use of intercept evidence in court'[1]. A review of this issue (the eighth review since 1993[2]) was commissioned and conducted by the Home Office, drawing on expertise from across the eight intercepting agencies and specialist legal advice. It was overseen and endorsed by a cross-party group of Privy Counsellors. This report summarises the work of the review and the Government's conclusions.

3. Under British law defendants must receive a fair trial under conditions that do not place them at a disadvantage compared to the prosecution. In practice this means the defence should have access to all material on which the prosecution relies, as well as any material which is capable of undermining the prosecution case or assisting the defence. The prohibition on using intercept as evidence is consistent with the right to a fair trial because neither the defence nor the prosecution can rely on intercept material.

4. For the use of intercept material as evidence to be consistent with a fair trial, *all* relevant material collected by an intercepting agency in the course of a given investigation would need to be retained to an evidential standard and made available to the defence.

5. All previous reviews of intercept as evidence have also recognised that an intercept as evidence regime must not significantly impede the operational activity of the intercepting agencies. The 2008 Privy Council review of intercept as evidence proposed nine 'operational requirements' which would need to be met by an intercept as evidence model. The present review recognised the continued validity of these operational requirements. They include the requirements that the intercepting agencies should select whether and for how long to retain intercept material in a given case and that the agencies should not be required to alter their operational monitoring or transcription arrangements.

6. The review concluded that the legal requirements for an intercept as evidence regime regarding the review, retention and disclosure of intercepted material cannot, as a matter of principle, be reconciled with the operational requirements set out in 2008, notably that the intercepting agencies should be able to determine how intercept material is transcribed and selected for retention. This assessment was confirmed by consideration of the specific models which have been previously

[1] The Coalition: Our Programme for Government – published 20 May 2010.
[2] A summary of previous reviews is attached at Annex C

proposed for an intercept as evidence regime, including models developed for the purpose of this review. The models are summarised in this report.

7. The review did identify a legally compliant model for intercept as evidence. This model would not be consistent with the agency operational requirements identified in 2008. The review considered the costs and benefits of this model. The cost would be between £4.25bn and £9.25bn over 20 years depending on assumptions about developing communications technology and usage, and technology costs. On some assumptions the model could lead to an increase in convictions; but on others the model could lead to fewer convictions than at present, due mainly to the compromise of sensitive techniques and the inability to prosecute cases where these techniques had been used.

8. Deriving highest benefit from an intercept as evidence model would be possible only if additional funding were made available to cover the additional costs. Under a flat funding scenario there would be no benefit from a legally compliant intercept as evidence regime because agency resources would have to be diverted away from operational work to staff and fund the intercept as evidence process.

9. The Government has concluded that although it is feasible to design a legally compliant intercept as evidence regime it would not be consistent with previous operational requirements, would incur significant costs and risks, and that the benefits would be uncertain. The Government therefore intends to make no change to the current arrangements which permit intercept material from this country to be used for intelligence purposes only.

10. The Government will keep under review any changes that might affect the conclusions of this review, including changes to the legal requirements that would reduce the burden of examination, retention and review on the intercepting agencies, and the development of new technologies that could reduce the need for manual translation and transcription of intercept material.

I. Introduction

11. In some countries, intercept material is used as evidence in criminal prosecutions. Successive Governments have sought to increase the number of successful prosecutions in terrorism and serious crime trials and have looked for viable ways to use intercept material as evidence in this country.

12. This Government committed to "seek to find a practical way to allow the use of intercept evidence in court."[3] This review began in January 2011, and is the eighth review since 1993.

13. The review was led by the Office for Security and Counter-Terrorism within the Home Office. It has been supported and endorsed by the intercepting agencies and other relevant organisations and departments. The review was overseen by the cross-party group of Privy Counsellors that undertook the 2008 review, comprising:

- Rt Hon Sir John Chilcot (Chair)
- Rt Hon Lord Archer of Sandwell, to November 2011 (Labour)
- Rt Hon Lord Howard of Lympne (Conservative)
- Rt Hon Sir Alan Beith MP (Liberal Democrat)
- Rt Hon Shaun Woodward MP, from November 2011 (Labour)

14. The role of the Advisory Group was to provide advice to officials as they carried out this work. It also offered advice to Ministers on the conduct of the review and its outcomes.

[3] The Coalition: Our Programme for Government – published 20 May 2010

II. Interception in the UK

What is interception?

15. Interception is the act of obtaining and making available the contents of communications sent via a telecommunications system or public postal service to a person who is neither the sender nor intended recipient. Warranted interception is a powerful tool for law enforcement and the security and intelligence agencies in tackling serious crime and terrorism. The use of interception by the state is limited to only a few agencies, for a limited range of purposes set out in legislation. It is subject to strong internal controls and independent oversight.

The legislation

16. Interception is one of the most intrusive powers available to the state and is subject to a strict authorisation and oversight regime. The use of interception is governed by the Regulation of Investigatory Powers Act 2000 (RIPA). Interception can only be used for purposes relating to serious crime, national security, or the protection of the UK's economic wellbeing when it relates to national security. . The power to intercept communications is limited to the following organisations:

- The Security Service;
- The Secret Intelligence Service;
- Government Communications Headquarters (GCHQ);
- The National Crime Agency;
- The Metropolitan Police Service;
- The Police Service of Northern Ireland;
- Police Scotland;
- Her Majesty's Revenue and Customs; and
- The Ministry of Defence.

17. To undertake interception, an agency must seek an interception warrant signed by a Secretary of State or a Scottish Minister. A warrant must consider the necessity and proportionality of the proposed interception and whether the information collected through interception could reasonably be obtained by other means.

18. The oversight regime provided under RIPA is intended to minimise intrusion and ensure that the intercepting agencies are acting lawfully. Agencies and warrant-granting departments are subject to scrutiny by an independent Interception of Communications Commissioner, whose findings are published annually. Redress for individuals who believe they have been wrongfully subjected to interception is provided by the Investigatory Powers Tribunal.

19. Safeguards are also in place to protect interception capabilities and the intelligence gathered through them. RIPA provides a framework for the protection of information collected through interception. It also creates a criminal offence for revealing that interception has taken place.

The uses of interception

20. Interception in the UK is used as a source of intelligence. That intelligence helps to identify and disrupt threats from terrorism and serious and organised crime and enable arrests. It supports the gathering of evidence and the identification of opportunities to seize prohibited drugs, firearms and the proceeds of crime. Interception can ensure that finite law enforcement resources – money and staff – are used to best effect. Detailed examples of how interception is currently used are set out in Annex A.

21. Law enforcement and intelligence agencies co-operate closely on interception in the UK, sharing the intelligence as well as skills, expertise and capabilities. The close relationship within the interception community is not replicated in other countries. It relies in part on the assurance provided by RIPA that sensitive capabilities developed by the security and intelligence agencies will not be revealed in open court at a trial.

Interception and the courts

22. With some limited exceptions, RIPA prohibits evidence gathered through interception from being disclosed in legal proceedings. This restriction applies only to material that is collected under a warrant. Interception obtained lawfully by other means, for example by consent, or undertaken in a foreign country, under that country's law, can be used as evidence in UK criminal courts.

23. There are some circumstances in which material collected under a warrant can be disclosed in legal proceedings. RIPA provides for intercept material to be adduced for the purpose of prosecuting offences under the act itself, such as unlawful interception. Intercept material can also be disclosed to the chair of a public inquiry or in proceedings before the Investigatory Powers Tribunal.

24. Interception can also be used in a small number of civil proceedings, which provide for material to be heard in closed session. These include certain tribunals, as well as Closed Material Proceedings held under the Justice and Security Act 2013. These are not criminal proceedings, and the subject will not ordinarily have access to sensitive material. The interests of the subject in such cases may be represented in closed elements by a security cleared special advocate. Civil proceedings in which intercept material may be used include:

- Special Immigration Appeals Commission proceedings
- Proscribed Organisations Appeals Commission proceedings
- Terrorism Prevention and Investigation Measures proceedings
- Financial Restrictions Proceedings under the Counter-Terrorism Act 2008
- National security cases before Employment Tribunals.

25. The bar on disclosure of intercept material in criminal proceedings helps to protect sensitive capabilities by preventing details of how intercept was obtained from being revealed in court.

III. Intercept as Evidence: Legal Requirements

26. Criminal trials in the UK must be fair. If intercept material were to be admissible as evidence in British criminal courts the defence must not be placed at a disadvantage. The review therefore considered in detail the tests that an intercept as evidence regime would need to satisfy in order to provide for fairness at trial.

27. Under British law defendants must receive a fair trial under conditions that do not place them at a disadvantage compared to the prosecution. This principle is reaffirmed by Article 6 of the European Convention on Human Rights (ECHR). Fairness at trial is ensured in relation to evidence in UK criminal trials by the Criminal Procedure and Investigations Act 1996 (CPIA). CPIA requires all relevant evidence available to the prosecution to be retained and made available to the defence ahead of trial.

28. The obligation on the prosecution to disclose material is not absolute: in any criminal proceedings there may be competing interests (such as protecting national security or sensitive investigative techniques) which need to be weighed against full disclosure. In some circumstances, such material may be withheld by the court. In such cases, the court must be satisfied that it is both strictly necessary to withhold that material and that the trial remains fair. This is known as the 'strict necessity' test.

29. The UK's current interception regime satisfies the strict necessity test. In the case of *Jasper* (2000), it was argued that the bar on disclosure of intercepted material in a UK court rendered the trial unfair. Ruling in favour of the UK, the European Court of Human Rights concluded that the prohibition on using intercept as evidence was consistent with the right to a fair trial, on the basis that neither the defence nor the prosecution was able to rely on intercept material.

30. Arrangements are also in place for the disclosure of intercept material to the court where necessary in the interests of justice, further ensuring the fairness of proceedings. This is known as the 'Preston' process. Retained material is reviewed by the prosecutor and, where necessary, a relevant judge, and action can be taken to secure the fairness of the proceedings (for example by making an admission of fact). However, the existence (or otherwise) of intercept material cannot be revealed to the defence. European case-law has confirmed that this is Article 6 compliant.

31. At present, any material which clearly points towards guilt or innocence is identified and reported to investigators, in order to develop a complete intelligence picture. But, the law enforcement or intelligence agencies are not required to examine, record, retain and review intercept material to the high evidential standard that would be necessary under an intercept as evidence regime. The safeguards afforded to material obtained under an interception warrant mean that intercept product is only retained as long as necessary for operational purposes.

32. For the use of intercept material as evidence to provide for fairness at trial, *all* potentially relevant material collected by an intercepting agency must be retained and made available to the defence. Like other forms of evidence, intercept would need to be searchable without imposing an unnecessary burden on the defence.

This would require the translation, transcription and cataloguing of all intercepted material in a given case. In a 2009 judgment the European Court of Human Rights[4] ruled that the destruction of intercept material before trial and without disclosure to the defendant was inconsistent with Article 6 rights, as the defence had valid reasons for seeking to examine the material.

33. If intercept as evidence were introduced in the UK without imposing full retention and disclosure obligations on the intercepting agencies, judges would need to take corrective action, for example, by staying the trial, to maintain fairness. Cases would be dropped and there could be fewer successful prosecutions.

[4] Natunen v Finland (Application No 21022/04) ECtHR Judgment of March 31 2009

IV. Intercept as Evidence: Operational Requirements

34. All previous reviews of intercept as evidence have sought to ensure that the potential benefits arising from the ability to use intercept material in prosecutions are not outweighed by disruption to operations of the intercepting agencies.

35. The 2008 Privy Council review of intercept as evidence proposed nine 'operational requirements' which would need to be met by an intercept as evidence model:

i. The intercepting agency should decide whether a prosecution involving their intercepted material shall proceed.

ii. Intercept material from the intelligence agencies should not be disclosed beyond cleared judges, prosecutors, or special (defence) advocates, except in a form agreed by the originator.

iii. Material intercepted (by any agency) through the use of sensitive signals intelligence ('Sigint') techniques should not be disclosed unless the Secretary of State was satisfied that disclosure will not put the capability and techniques at risk.

iv. No intelligence or law enforcement agency should 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).

v. No intelligence or law enforcement agency should 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).

vi. Intelligence and law enforcement agencies should 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.

vii. Law enforcement agencies should 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.

viii. 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 should be subject to the same disclosure obligations as other intelligence intercept.

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

36. The detailed assessment of the nine requirements produced by the Privy Council group in 2008 is at Annex B. The review concluded that the legal

requirements of CPIA regarding review, retention and disclosure could not, as a matter of principle, be reconciled with the operational requirements set out above, notably that the intercepting agencies should be able to determine how intercept material is selected for retention and transcription.

V. Models for Intercept as Evidence

37. The review assessed a range of proposed intercept as evidence models, including: those developed by previous reviews; those employed in other jurisdictions; and two new models, developed in the course of the review. The review also considered whether changes could be made to operational practice to reduce the resource burden associated with these models. This section summarises these models. Section VII assesses their relevance.

Previous models

38. Each of seven previous reviews of intercept as evidence has tried to reconcile legal and operational requirements. The models took one of three approaches:

- Limiting the operational impact by undertaking some interception in line with CPIA (with intercept material usable as evidence), but leaving much (or most) interception (and interception practice) unaffected. Examples of this approach include the Dual Warrant, Triple Warrant, Two Warrant and Lord Carlile models.

- Changing legal practice by amending CPIA practice in order to protect sensitive capabilities from disclosure. Examples of this approach include the Public Interest Immunity Plus model and Judicial Oversight and Examining Magistrates variants of this.

- Changing both legal and operational practice. Examples include the 'Keys to the Warehouse' and Review Pursuant to Defence Requests models.

39. A summary of models previously considered is set out below. A detailed analysis of each is included at Annex D.

Approach	Summary
Reviews 2, 3, 4a, 5 and 6: 1995, 1997-98, 1998-99, 2002-03 and 2003-04	
Dual Warrant model	Tried to reduce operational impact by creating 'evidential warrants' and 'intelligence warrants'. Intercept material collected under the former would be admissible in court. Interception under intelligence warrants would not.
Review 6: 2003-04 & follow up to January 2005	
Triple Warrant model	Tried to address operational impact by allowing investigators to apply for evidential warrants in a small number of cases.
Internal work: 2005	
Pre-Trial sift	Tried to protect sensitive material by providing the defence with a summary of intercept material agreed by the judge.
Review 7: (a) Privy Council 2007-2008; (b) implementation to December 2009	
Two Warrant	Tried to reduce operational impact (like the 'dual warrant'

model	approach). Law enforcement agencies would apply for evidential warrants. Security and intelligence agencies would seek intelligence warrants.
Model proposed by Lord Carlile	This would provide the Attorney General or Director of Public Prosecutions with the power to designate investigations as 'interception cases' where appropriate in the interest of justice. These would be run on a CPIA-compliant basis.
Public Interest Immunity (PII) Plus Model	Tried to reduce operational impact by protecting existing agency examination, retention and review practice and departing from that required under CPIA.
Review 7 (c): 2010 Scoping analysis and report to the Prime Minister	
Mandatory Judicial Oversight of Deletion / Examining Magistrates	These models sought to address the flaws in the PII Plus model, by subjecting retention and deletion decisions to enhanced judicial supervision.
'Keys to the Warehouse'	This model sought to reduce costs of examination and review by placing responsibility for the latter on the defence.
Review Pursuant to Defence Requests	This sought to mitigate costs of examination and review by placing responsibility on the defence to identify when exculpatory communications took place.

International models

40. The use of intercept material as evidence is common across a range of overseas jurisdictions.

41. The most recent review of intercept as evidence[5], in 2008, looked at three common-law countries with adversarial legal systems (the USA, Australia and Canada) and three EU countries with inquisitorial systems (France, the Netherlands and Spain). That review found that the overseas experience was of limited value in considering the issues raised by the use of intercept material as evidence in the UK. The present review reconsidered these findings.

New models

42. Building on previous efforts, the present review went on to develop two new models: a model in which intercept material would not be admissible if gathered using techniques or capabilities that would be compromised if revealed in open court (the 'Non-Sensitive' model); and a model in which the Government would permit the use of intercept material in certain cases where it was in the interests of justice (the 'Interception Case' model). Each of these built on one of models developed by previous reviews.

[5] Privy Council Review of Intercept as Evidence Report, 30 January 2008.

The Non-Sensitive model

43. This model makes a distinction between 'evidential' and 'intelligence-only' interception according to whether intercept material was collected through sensitive techniques or capabilities. The legal viability and operational practicability of this model depends on:

- the ability to define and manage the boundary between non-sensitive and sensitive interception;
- the proportion of non-sensitive interception; and
- the examination, retention and review burden incurred by 'sensitive' interception.

The Interception Case model

44. This model would provide the Attorney General or Director of Public Prosecutions with the power to designate some investigations as 'interception cases', in which intercept material could be used in trials where appropriate in the interest of justice. These cases would be run on a CPIA-compliant basis. Interception in support of other investigations would be undertaken in line with existing processes and could therefore not be used in court. The model is summarised at annex E.

45. The intention would be to ensure that operational burdens from an intercept as evidence regime remained manageable. This approach would of course limit the potential benefits of introducing intercept material as evidence in a relatively small subset of cases.

Reducing the resource burden

46. The review also considered three options for reducing the resource burden associated with an intercept as evidence regime:

- Limiting use of intercept material as evidence to terrorism-related cases only.
- The use of interception 'excerpts' only. The prosecution would be able to use intercept where there was an overwhelming public interest or a compelling stand-alone item of intercept material.
- Limiting full disclosure requirements to cases in which intercept forms part of the prosecution case.

VI. Reconciling Legal and Operational Requirements

47. The review found that none of the models set out at section VI above could meet both the legal and 2008 operational requirements specified for an intercept as evidence regime. Most models would not be legally compliant. Those which were legally compliant could not be implemented without changes to agency operational practice.

Assessment of possible models

48. Only one previously considered model (Pre-Trial Sift, referenced at paragraph 39 above) was found to be consistent with the legal requirement of fairness at trial. It would, however, require significant changes to the operational work of the intercepting agencies.

49. The other models developed by previous reviews were found to have further disadvantages, such as introducing greater complexity at trial or reducing the ability to protect sensitive material, techniques or capabilities. These findings are reinforced by the lessons learned from a series of mock trials run by law enforcement and the intelligence agencies in 2009 using the PII Plus model. That experience highlighted the risk of exculpatory material being deleted under that model, potentially rendering any trial unfair.

International models

50. The 2008 review concluded that while many countries have intercept as evidence models which operate within their own legal contexts, the models would not meet UK legal requirements, or would not meet the operational requirements of the intercepting agencies.

51. Approaches adopted in the EU are based on inquisitorial legal systems in which disclosure obligations are more limited than in the UK, where the adversarial system places greater emphasis on determining the facts of the case at trial. Other common law countries are more relevant, but important differences remain, including greater separation of law enforcement and intelligence agencies, and the approach to plea bargaining.

52. The Republic of Ireland, which like the UK, has both an adversarial legal system and shared case law concerning fairness at trial, does not use intercept as evidence and has instead adopted the practice of using intercept material for intelligence purposes only.

New models

53. The Non-Sensitive model (paragraph 43, above) was found to be consistent 'in principle' with Article 6 of the ECHR, but it would cause significant difficulties. The model would only work if it were possible to distinguish between sensitive and non-sensitive capabilities. Given the way in which interception technology and techniques have evolved over time (often building on the same basic capabilities), it may not be

possible to draw such a distinction. Even if an artificial distinction were made, a significant number of cases might involve intercept material that was considered sensitive. All material in those investigations would still be subject to full CPIA examination, retention and review obligations.

54. The review also found that the Interception Case model (paragraph 44) would not be consistent with Article 6 of the ECHR. The model would likely fail the strict necessity test for withholding material from the defence. It would also provide the Executive with discretion over whether a certain class of evidence could be excluded from a trial.

Reducing the resource burden

55. None of the options considered by the review to reduce the resource burden associated with an intercept as evidence regime (and therefore more closely meet the operational requirements at paragraph 35, above) was consistent with fairness at trial:

- Limiting use of intercept material as evidence to terrorism-related cases only would not be permitted under British law. If intercept material were evidential, it would need to be made available to the defence in any case where interception contributed to the investigation.

- The use of interception 'excerpts' only would fail to satisfy the requirement for fairness at trial. This reflects the European Court of Human Rights' 2009 Natunen judgment (paragraph 32, above).

- Limiting disclosure to cases in which intercept forms part of the prosecution case could lead to trials being halted in cases where interception had contributed to an investigation, but was not then used by the prosecution.

Conclusion

56. The review could not identify an intercept as evidence model which would meet legal and operational requirements (set out at section III and paragraph 35).

57. Meeting the requirements of fairness at trial and the CPIA would require intercept material to be treated in the same way as other forms of evidence. In order for it to be searchable by the defence without imposing an unnecessary burden, the intercepting agencies would be required to translate, transcribe and catalogue significantly greater volumes of intercept material than is currently the case. All intercepting agencies would need to:

- Listen in full to all intercepted material collected in support of a criminal investigation; and

- Produce a basic 'gist' or a fuller 'summary' of the content of the communication, which would then need to be indexed.

58. The index, gists and summaries (and equivalents for non-voice communications) would be retained by the intercepting agency and would form the basis for a meaningful pre-trial disclosure review for exculpatory material. Intercept product would also be retained with segments transcribed in full, as necessary, for evidential or disclosure purposes.

59. Under current practice, intercept material is retained only to the extent necessary for intelligence purposes. Investigators will often only be provided with relevant details and material will rarely be transcribed or retained.

60. Different legal systems make the admission of intercept as evidence easier in some other countries than it would be here. But the review concluded that the models used in these countries had limited relevance to the UK.

VII. Changing Operational Requirements

61. The review assessed the costs and benefits of introducing intercept as evidence in a way that satisfied legal requirements irrespective of the operational requirements of the intercepting agencies.

62. The most reliable way of ensuring that an intercept regime is compliant with Article 6 and the CPIA would be to treat intercept material like any other form of evidence, where necessary and practical using public interest immunity to protect sensitive material. On that basis, the review assessed the costs and benefits of simply repealing the current prohibition on intercept as evidence.

63. Repealing the current prohibition would require that all intercepted voice communications was analysed in full by the intercepting agencies. Voice material would be indexed and a basic 'gist', or a fuller 'summary' of the content of the call produced. Non-voice material, such as email, would be easier to summarise and index. The index, gists and summaries would be retained by the intercepting agency and form the basis of a pre-trial disclosure review for exculpatory material. Raw and processed intercept product would also be retained for evidential or disclosure purposes.

64. The operational impact of introducing this model would be significant. All agencies would need to collect intercept material in line with CPIA examination, review and retention obligations. This would significantly increase the translation and transcription burden. It would also require the security and intelligence agencies to establish processes for the production and dissemination of evidential material. It would also potentially lead to the disclosure of sensitive capabilities in order to meet CPIA obligations; in order to reduce this risk, prosecutions may need to be dropped.

65. The agencies told the review that they face challenges recruiting sufficient numbers of staff with the required skills to translate, transcribe and assess intercept material and that it may not be possible to recruit the staff to process the material in the manner required by an intercept as evidence regime. This may make it impossible to maintain current interception volumes. If a regime was introduced with flat funding, and capacity was therefore less, staffing requirements would be more feasible.

66. The review considered whether change of this scale could be justified by an analysis of costs, benefits and risks.

VIII. Costs and Benefits of Intercept as Evidence

The Cost-Benefit Analysis

67. An intercept as evidence regime would impose costs on the intercepting agencies, the Crown Prosecution Service (CPS) and the wider Criminal Justice System. Benefits may include more prosecutions and convictions.

68. The cost-benefit analysis considered two funding scenarios: 'full funding' (i.e. additional funding being provided to meet any additional costs) and 'flat funding' (which assumed no extra funding, with the additional costs being absorbed within existing agency budgets). Full funding would maximise potential benefits and protect other interception agency activities but would have financial consequences for wider Government spending. Flat funding would limit the additional costs but would mean that interception volumes would be significantly reduced.[6] It would therefore have a significant impact on the work of the intercepting agencies.

The costs of intercept as evidence

Fully funded

69. Working with Home Office experts, including economists, and with the agencies, the review developed an estimate of the costs of an intercept as evidence model. Fully-funded implementation of the introduction of intercept as evidence would have a total present cost of between £4.25 -£9.25bn[7] over the 20 year period, of the cost- benefit analysis. This includes the one off and annual costs over the first twenty years. The wide range of costs reflects the scope for development in the technologies that support examination and transcription.

70. The costs at the higher end of the range were primarily driven by the assumption that the volume of communications undertaken by suspects would increase by 200% over the 20 year period of the cost benefit analysis, reflecting an assumed growth in internet use by people under investigation, and the use of multiple means of communication. This cost estimate does not assume an increase in the numbers of people whose communications would be intercepted.

71. The key cost is for the staff required for examination, notation and review. For voice interception this would involve analysing calls in full and producing 'gists' and 'summaries' to enable a meaningful pre-trial review for exculpatory material. It was assumed that some of the processes involved – e.g. for some non-voice material such as emails etc – could be partially automated. However it is unlikely that tools such as automatic translation and transcription would reach the levels of evidential reliability required in order to remove the need for manual input for voice communications. The need for additional staffing also creates additional accommodation costs.

[6] This assumes no change in spending on other work undertaken by the intercepting agencies.
[7] Net Present Cost over 20 years, excluding criminal justice systems costs related to increases/decreases in the number of prosecutions and convictions.

72. The review concluded that technology costs were much less significant. Considerable redesign and major upgrades would be required to enable systems to operate to evidential standards and to allow processing and retrieval of much greater volumes of retained material. However, the price of storage is expected to continue to fall rapidly.

73. An example of the break down of costs (excluding criminal justice system costs) across flat and high communications growth assumptions for intercept as evidence can be found at Annex F.

Flat funding

74. The flat funding scenario would mean no additional spend: the cost of operating an intercept as evidence model would be absorbed within agencies' existing budgets. But there would necessarily be significant operational consequences: the increased resource burden would mean either that a very large amount of other agency activity was dropped to fund intercept as evidence or that interception would be available for many fewer investigations – or both. This is considered further below.

Benefits

75. The main potential benefit from the use of intercept material as evidence would be more convictions, additional to those already secured from the use of interception for intelligence purposes. It is not and will not be possible to pilot the use of intercept as evidence to test this hypothesis: if intercept were introduced in pilot cases, it would not be possible then to reinstate the prohibition on the use of intercept material in open court because the defence would be able to challenge the claim that it was strictly necessary to exclude intercept material from criminal proceedings.

76. Making benefits assessments in this area is necessarily challenging. Estimates were therefore generated for a range of assumptions. These estimates should be seen as illustrative rather than precise forecasts. The potential for additional convictions would be influenced by whether implementation was fully funded or flat funded. The possible implications for other agency objectives (such as drug and cash seizures) also need to be considered given increased resource burdens.

77. The methodology used by the review for estimating these potential benefits was based on a two stage process:

i. First estimating the maximum number of additional convictions that could be gained from the use of intercept as evidence, based on the number of intercept warrants issued; and then

ii. Testing this maximum figure against factors that could reduce the number of successful prosecutions, including the ability to prove the attribution or authentication of intercept material in court.

78. Further detail on the model used to estimate benefits is set out at Annex H.

79. There are economic and social costs associated with crime. Any additional convictions through the use of intercept as evidence would therefore have economic and social benefits. Not only would those engaging in criminal activity be brought to justice, but convictions could prevent future crimes being committed as well as acting as a deterrent for other potential criminals. The review concluded that it was not possible to quantify the benefit at this stage.

80. Having tested a number of scenarios using different assumptions, the review noted that there would be a wide range of possible outcomes from an increase of up to 170, to a decrease of up to 200 successful prosecutions each year. This reflects the fact that, though intercept material may benefit the prosecution, intercept techniques might be compromised and disclosed during that process and would need to be protected. The number of convictions would therefore be affected by:

- **the proportion of intercept material which would be sensitive**. This material could not be used in court without a significant risk of targets learning how to evade current techniques and capabilities or learning about ongoing operations. Such material would therefore not be admitted in court, reducing the amount of evidence that could be relied on by the prosecution. The review therefore tested a number of options, including scenarios where the proportion of sensitive intercept material was high or low.

- **the ability to protect sensitive capabilities**. Public Interest Immunity (whereby the Government may apply to withhold sensitive material) would not always provide for the protection of sensitive capabilities. In some instances the only way of protecting sensitive capabilities would be to avoid bringing charges or dropping them in the course of the trial. The review again tested a range of assumptions about how often this might occur.

81. The cost-benefit analysis showed that:

i. only one of the scenarios generated a significant net increase in convictions;

ii. small changes in the key assumptions (such as the proportion of material considered sensitive) would have an impact on net benefit;

iii. the number of abandoned prosecutions would be likely to grow as a result of the increasing volume of internet communications, which the agencies assess increases their reliance on sensitive capabilities.

82. The introduction of intercept as evidence may therefore result in an increase in convictions. But securing and sustaining a significant net gain may be hard to achieve.

83. In all the scenarios tested, flat funded implementation would lead to between 360 and 540 fewer convictions each year[8] as agencies reduced interception to manage the additional costs of examination, retention and review.[9]

Costs and benefits: conclusion

84. The review concluded that a fully funded intercept as evidence model could lead to a significant increase in the number of successful prosecutions. But an intercept as evidence model would necessarily lead to a change in agency operational practice and over twenty years would cost between £4.25 and £9.25bn. There could be a reduction in the number of successful prosecutions as a result of the compromise of operational techniques.

85. Without significant additional funding any legally compliant intercept as evidence regime would certainly lead to fewer prosecutions and to a reduction in the use of intercept to support agency operational work.

[8] Annual 'steady-state' change relative to 'intercept as intelligence' baseline.
[9] The implications of partial funding were also explored. However, even on the basis of providing 50% of the additional funding required it remains likely that less interception would mean that the number of successful prosecutions would be significantly lower than at present.

IX. Conclusion

86. The review concluded that it is not possible to find an intercept as evidence model that is consistent with both legal requirements of fairness at trial and the operational requirements set out in the 2008 Privy Council review.

87. It would be possible to identify a legally compliant intercept as evidence model which would not be consistent with the operational requirements identified in 2008. However, that model would incur significant additional costs. With anything less than full funding it would not lead to an increase in convictions. With full funding there would remain increased risks from the disclosure of sensitive techniques which might reduce the benefits; and it may not be feasible to recruit the staff required.

88. Having considered the findings of the review the Government believes that the costs and risks of using intercept as evidence are disproportionate to the assessed benefits and therefore does not intend to proceed to an intercept as evidence model at this stage.

89. Any developments in either domestic or ECHR case law that would reduce the review, retention and disclosure obligations on the intercepting agencies would have a significant impact on the findings of the review, reducing costs and increasing benefits.

90. The development of new technology could substantially reduce the need for manual examination, notation and review of intercept material. This could also reduce the requirement for additional staff under an evidential system and has the potential to make the system much less burdensome.

91. The review considered neither of these scenarios to be likely in the foreseeable future. Any amendment to review or disclosure practices would require substantial changes to both domestic and European law and would be at odds with recent rulings, which have emphasised the importance of equality of arms between the defence and the prosecution.

X. Next Steps

92. Based on the outcome of the cost benefit analysis, the review concluded that intercept as evidence should not be introduced at this time. However, the Government will keep this position under review.

ANNEX A: CASE STUDIES OF THE CURRENT USE OF INTERCEPT AS INTELLIGENCE

Serious Organised Crime Agency (SOCA) Case Studies[10]

Case 1

A criminal investigation into a UK-based organised crime group involved in the importation of Class A drugs from South America.

Interception assisted in identifying the command and control structure of the group and their associates in other European countries. It identified individuals responsible for facilitating the supply of drugs and also those involved in establishing front companies for importing legal goods. Intercept provided intelligence on the *modus operandi* employed by the group, the dates and location of the importation, and the storage place of a series of drug shipments.

This resulted in the arrest of UK-based members of the group and their co-conspirators overseas, as well as the seizure of significant quantities of Class 'A' drugs, foreign currency, firearms and ammunition. Intercept material provided key intelligence which was pivotal in building an evidential case and ended in the successful prosecution of the defendants. It also served to enhance SOCA's working relationships with overseas partners involved in the investigation.

Case 2

A criminal investigation into an organised crime group based in the south east of England involved in acquiring, supplying, and storing firearms in the UK.

Interception provided intelligence on the structure of the organised crime group, its methods of working, and the types of crime it was involved in. It helped to identify the types of firearm and the locations where the weapons and ammunition were stored. This led to the seizure of weaponry which ranged from handguns to automatic weapons, as well as significant quantities of ammunition. It also provided intelligence on turf wars with other groups operating in the area, which was critical to operational planning.

The intelligence provided by intercept was developed further and helped to identify those responsible for the wholesale supply of firearms in Europe. It also revealed changes to the structure of the group and its weaknesses, enabling SOCA to re-focus the investigation.

The result was the successful prosecution of a significant number of gang members involved in the supply and distribution of firearms.

[10] The Serious Organised Crime Agency was replaced by the National Crime Agency on 7 October 2013, during the course of this review.

Metropolitan Police Service Case Studies

Case 1

A criminal investigation into a pattern of escalating violence between a number of rival organised crime groups, including street gangs linked to the London drug economy, operating across the capital.

Intelligence derived from interception indicated a conflict between organised crime groups as each sought to control a greater section of the drugs market. The intelligence suggested the use of firearms by the groups. This prompted immediate steps to tackle the group, with the intention of dismantling the network, disrupting the supply of Class A drugs, preventing further loss of life and arresting those involved. The operation also targeted individuals directly involved in gun possession and crime whilst disrupting other criminal activities such as small scale drug dealing, acquisitive crime and serious assaults.

Intercept material identified the individual co-ordinating the sale of significant amounts of Class A drugs, led to the location of his safe storage premises, and identified senior gang members involved in the supply chain. It also enabled junior gang members to be identified as couriers of the drugs to numerous locations across London, the Home Counties and beyond, including the method and timing transport. Interception also revealed that the head of the organised crime group was conspiring with others to shoot a rival. This led to an armed stop of the target whilst he was *en route* to the hit location. He was found to be in possession of a loaded firearm and arrested.

The primary operation led to the collapse of the network operating across London and the Home Counties. During the course of the operation, intelligence from interception led to the seizure of over 40 firearms, in excess of 200kg of Class A drugs, the seizure of over £500,000 of cash and over 100 arrests.

Case 2

A criminal investigation into a London-based money laundering network, linked to several organised crime groups that were responsible for a major share of criminal activity across London.

An operation was launched in partnership with HM Revenue & Customs to identify the proceeds linked to the groups' criminal activities and to deny them funds. The police had identified that a considerable quantity of cash was being laundered on a regular basis by a relatively small group of criminals. The launderers were identified as working for multiple crime networks and making significant profits. However, traditional policing methods were unable to provide details of how the network ran their business.

Intercept material indicated the method by which the laundering network was moving funds between accounts. This led to the covert interception of high value cash transactions, depriving the organised crime groups of their profits and diminishing their ability to complete criminal transactions.

During the operation, cash in excess of £3 million was seized. Intercept intelligence indicated that a number of criminal enterprises had collapsed and a number of targets had been forced to cease their activities due to a lack of funding.

HM Revenue & Customs Case Study (HMRC)

Multi-trader intra-community (MTIC) fraud is estimated to cost the exchequer approximately £750 million annually. The fraud typically comprises a scheme involving a number of participants which is set up with the sole purpose of defrauding the public purse. For example, an organised crime group acquires a VAT registration number in the UK for the purposes of purchasing goods free from VAT in another EU member state. The goods are imported into the UK and sold at a VAT inclusive price. The UK company selling the goods will then 'go missing' without paying the output tax due to HMRC. The criminally obtained funds will be laundered through a complex network of financial transactions involving bank transfers and cash movements in the UK and overseas. In practice, MTIC fraud will involve complex layers of companies performing different functions in an effort to conceal the fraud and to thwart investigation and compliance activity.

In one particular operation, supported by interception, a total of £3.2 billion in VAT repayments was withheld from criminal groups fraudulently trading in mobile telephones and computer chips. Interception was also critical in identifying the bank of first choice for laundering the proceeds of the crimes. Working with international partners, HMRC was able to prevent the distribution of assets to the criminal gangs. The scale of the criminal conspiracy and related laundering operation is illustrated by the fact that over $200 million of MTIC funds have been frozen and are the subject of criminal and civil action.

Since HMRC started using interception to support investigations into MTIC fraud, the level of attempted fraud has reduced substantially from an estimated high of £5 billion in 2005/2006 to an estimated current figure of £750 million.

ANNEX B: THE 2008 PRIVY COUNCIL REPORT - NINE OPERATIONAL REQUIREMENTS

B1. The Privy Council Review of Intercept as Evidence, published in January 2008, stated that any intercept as evidence regime should have to meet nine operational requirements, which the review judged to be necessary in order to protect the public and national security. These requirements guided their work and the subsequent attempts to assess the viability of the model they recommended. The review, published in December 2009, set out these requirements in more detail with accompanying analysis and comment. This is reproduced below.

Operational Requirement	Application and Comment
1. The intercepting agency shall decide whether a prosecution involving their intercepted material shall proceed.	The decision whether to prosecute a case or not remains with the relevant prosecuting authority. The decision whether to provide intercept evidence rests with the intercepting agency. Clearly the availability or otherwise of intercept will impact on the relevant prosecuting authority's assessment of case credibility and decision on whether or not to proceed. However, the appropriate action will be taken if, in the course of the trial, the intercepting agency believes that sensitive intercept material is at risk of exposure. This includes material, capabilities or techniques whether being relied on by the prosecution or unused. "Appropriate action" includes action (such as the withdrawal of certain charges) up to and including the withdrawal of the whole prosecution, as required by the intercepting agency to ensure protection of its material, capabilities or techniques.
2. 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.	All retained intercept product originating in the intelligence agencies would (in principle) be subject to the Criminal Procedure and Investigations Act 1996 (CPIA). However, sensitive material, capabilities or techniques would be protected by Public Interest Immunity (PII), with only judges, cleared prosecutors and special (defence) advocates having access to the material and to the capabilities that it would reveal. The originating agency would need to be content with the form of any wider dissemination of material (including that brought forward as evidence) in open court whether in its original form or otherwise "gisted".
3. Material intercepted (by any agency)	Any disclosure of intercept acquired through

through the use of sensitive signals intelligence ('Sigint') techniques shall not be disclosed unless the Secretary of State is satisfied that disclosure will not put the capability & techniques at risk.	sensitive Sigint techniques (including its use as evidence) would require the prior approval of the Secretary of State, confirming that capability and techniques would not be jeopardised.
4. 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).	The agency selects what material to retain and for how long in accordance with its requirements (operational or, should it so decide, evidential). They cannot be required to retain material against the possibility of potential evidential relevance.
5. 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).	The agency cannot be required to alter its operational monitoring or transcription requirements. The courts, ultimately, determine what constitutes evidential standards. However, the agencies retain the right to determine whether to provide material to these standards (e.g. to cease to do so in response to changing standards).
6. 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.	Agencies will be able to switch between evidential and intelligence interception without difficulty should it be necessary in a specific operation. More generally operations must not be impeded or otherwise impacted by the requirements of intercept as evidence.
7. 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.	Existing law enforcement agency ability to undertake, retain and protect long-term strategic intelligence will not be impaired. As now, it will be possible to switch between strategic and tactical intercept without difficulty, should it be necessary in a specific operation, with the product being handled accordingly.
8. 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.	Neither the current operational tasking of the intelligence agencies by the law enforcement agencies, nor the consequent sharing of product would be impeded by the introduction of intercept as evidence. However, any such product would be subject to the same agency veto safeguards as set out in operational requirements 1, 2 and 3, above.

9. At trials (whether or not intercept is adduced as evidence) the defence shall not be able to conduct successful 'fishing expeditions' against intercept material alleged to be held by any agency.	Both operational needs (capabilities and techniques) and legal process must be protected from speculative defence inquiries for intercept material (above and beyond that disclosed with the agreement of the intercepting agency at the start of the trial though the usual Criminal Procedure and Investigations Act 1996 processes). This includes those dealt with under the PII Plus processes (e.g. operational requirements 1 to 3 above).

ANNEX C: INTERCEPT AS EVIDENCE REVIEWS 1993-2010

Review Scope	Findings
(1) IOCA (Interception of Communications Act, 1985) Section 9 Group Review: December 1993 –October 1994	
Covered: overseas experience & value in court. No specific models were developed.	That next steps focus on how rather than whether change should take place.
(2) IOCA Review Team: May to September 1995	
Considered the: wider changes on disclosure; safeguard of processes; need to preserve more material; likely effectiveness in court; and possible intelligence losses. Compared (option 1) 'single tier' & (option 2) 'two tier' models. The latter was seen as preferable.	Not to proceed at present, as 'clear and convincing case' not fully made & reflecting agency concerns. Could be re-examined once wider disclosure changes bedded in and review of IOCA complete.
(3) Review of the IOCA: June 1997 to February 1998	
Undertaken within wider IOCA review. Three options considered: options 1 & 2 above & the status quo; proposals from Lord Lloyd and David Trimble also assessed. Arguments set out for & against (e.g. exposure of capability; evidential value; overseas; impacts on CSPs; cost & resources).	No recommendation made in the report as consensus not possible.
(4a) Harrington Report (b) international follow-up 1998-99	
(a) Key issues: (i) security; (ii) Communication Service Provider co-operation; (iii) practical & resource concerns. Two (dual and single) tier models developed. Ways of minimising the 'transcription'; burden (handing tapes to the defence; legislative limitations; judicial oversight) considered but deemed impractical. **(b)** International follow-up involved visiting four EU and three common law jurisdictions noting differences in inter-agency cooperation and legal structures.	**(a)** The legal viability of a two tier model was uncertain; a single tier model would be more legally robust but would create serious resourcing problems. **(b)** Concluded that overseas examples *gave no reason to doubt the... decision to maintain the prohibition...*'
(5) Home Office review: January 2002 to January 2003	
Home Office review in liaison with Northern Ireland Office, based on a 'dual warrant' model. Arguments for: scope for more prosecutions & technical feasibility. Arguments against: risks to current prosecution success, exposing techniques/capabilities, inter-agency cooperation; problems defining the evidential/intelligence boundary; the resource impact resulting in fewer operations.	Little support for a simple repeal of RIPA Section 17 or for a 'dual warrant' approach; evidence suggested that for counter-terrorism (CT) the intelligence benefits far greater than possible evidential gain; the dual warrant model was deemed at the 'outer edge' of ECHR compatibility but further assessment was thought likely to be helpful.
(6) PM requested review: July 2003 to July 2004, & follow-up to January 2005	
Looked at: overseas experience (intercept as evidence valuable, but bureaucratic; less inter-agency cooperation than in the UK; general concern about new technology); legal issues (a 'dual warrant' approach, potentially ECHR compatible, then morphed into 'triple warrant' model); case-studies (including 15 live operations); costs (£20m per annum if only 5% of law enforcement agency warrants were evidential).	'Dual warrant' model not viable due to resourcing impacts. The 'Triple warrant' model was a possible alternative but not fully explored and unlikely to 'completely assuage' concerns. Intercept as evidence unlikely to help against the most serious criminals or CT targets. Technological developments likely over time to reduce share of evidential material.

(7a)Privy Council review: July 2007 to January 2008 (b) Implementation: to December 2009; (c) Further scoping: to March 2010	
(a) Privy Council review considered: overseas experience, emerging technology, and three (Two Warrant; Lord Carlile and PII Plus) legal models. **(b)**Work programme centred on Design, Build and Test of the 'PII Plus' model. **(c)** Assessed whether: judicial oversight; full retention and alternative means of review; and new technology might address problems.	**(a)** Recommended PII Plus model, subject to nine 'operational requirements'. **(b)** Concluded that the model would not be legally viable. **(c)** Concluded that first and third of these unlikely to help; the second was at best very problematic.

ANNEX D: PREVIOUS LEGAL MODELS

Approach	Finding
Considered in 1995, 1997-98, 1998-99, 2003-04 reviews	
Dual Warrant model	Sought to mitigate cost by distinguishing between 'evidential warrants' for interception which would be admissible in court, and 'intelligence warrants' where it would not be and where operational practice would remain as now. One variant (leaving choice of 'evidential' or 'intelligence-only ' warrant at agency discretion or based on resourcing considerations), was **not legally viable** because it violated **fairness at trial** (Article 6 of the ECHR) requirements, in particular failing the 'strict necessity' test and risking agencies unfairly 'cherry-picking' the warrant used. A second variant **would be legally viable** – the non-sensitive model - as the distinction would be drawn on objective technical grounds – e.g. the sensitivity of interception. This would not reconcile the requirements for any model to be legal compliant (examination, retention and review) and current **operational requirements** due to the likely burden of operating 'evidential warrants'.
2003-04 review	
Triple Warrant model	Sought to address the resourcing problem identified in the dual warrant model, by carving out a small 'intercept as evidence - niche', leaving remaining agency interception practice intact. Judged at the time to be **capable of being ECHR Article 6 compliant**. But **it was found not to be practicable**. Subsequent developments strongly suggest that it would **fail to reconcile legal** and **operational requirements**: in particular the *Natunen v Finland* ECtHR case and evidence from 'live testing' the PII plus model (see below) on the risk of potentially exculpatory material being deleted.
Internal work during 2005	
Pre-Trial sift	Sought to protect sensitive material by providing a judicial pre-trial hearing to examine sensitive material and produce a statement of open evidence to be used in criminal trials – while protecting the sensitive intercept itself. The model, being centred on the protection of sensitive material, **would not address** the need to **better reconcile legal** and **operational requirements as it focused on allowing more intercept to be used in proceedings, rather than reducing examination, retention and review requirements.**
Privy Council review 2007-2008	
Two Warrant model	A 'dual warrant approach, with the 'evidential/intelligence' boundary based on which organisation was undertaking interception. This is **not consistent 'in principle' with the requirements of Article 6** because it does not meet the 'strict necessity' criteria. Even if it had been viable the consequent **resourcing burdens** would still have fallen in full on the **law enforcement agencies** and probably on the **Security Service** as well.
Lord Carlile model	In this model intercept material would, if retained, be admissible as evidence where 'necessary in the interests of justice' in a specific case. The 'interests of justice' test applied by the Attorney General or Director of Public Prosecutions would fail the ECHR's 'strict necessity' test for withholding material. The Government would in effect be deciding whether a certain class of

	evidence would be excluded from trial.
Public Interest Immunity (PII) Plus Model	Recommended for development by the Privy Council review, it was intended to protect **resourcing** by protecting existing agency examination, retention and review practice and departing from that required under the Criminal Procedure and Investigations Act 1996. Compatibility with **ECHR Article 6 rested on** the ability to **identify potentially exculpatory material at the point of interception.** Senior independent legal practitioners found that this would not be possible. Subsequent **ECtHR case law (*Natunen v Finland*) confirms the need for full retention in an evidential regime.** In order to try and increase legal robustness at trial, two variants were explored: mandatory judicial oversight and examining magistrates.
Scoping analysis spring 2010	
Mandatory Judicial Oversight of Deletion Examining Magistrates	Sought to address the Article 6 flaws in the PII Plus model, by subjecting retention and deletion decision to enhanced judicial supervision. **Neither could address the problem of identifying potentially exculpatory material at the point of interception,** the likely result being the **mandating of much fuller levels of retention,** consistent with the Criminal Procedure and Investigations Act 1996 but **at variance with the operational requirements.** The Examining Magistrates model (which is based on the French system, but would start at the beginning of an investigation and would place the investigation in the hands of an Examining Magistrate) would additionally require major, impractical changes to law enforcement and interception agency operations and would in consequence violate many of the other operational requirements.
'Keys to the Warehouse'	Sought to mitigate costs of examination and review by placing responsibility for the latter on the defence. **To ensure consistency with fair trial requirements the defence would have to be provided with sufficient resources to undertake the necessary review itself, negating the intended resource saving.** Protection of sensitive material would be very difficult. Full retention of material would be required. Trial length and complexity would be greatly increased.
Review Pursuant to Defence Requests	Sought to mitigate costs of examination and review by shifting responsibility from the prosecution to the defence to identify when exculpatory communications took place. It was deemed **unlikely to breach Article 6 of the ECHR at a systemic level** but the **practical difficulties** that flow from complying in any given case **were thought likely to be substantial.** So while offering **scope in principle to mitigate examination and review costs,** it would **require full retention** and **in practice shift examination** and review **burdens to later in the process,** i.e. during the trial itself rather than prior to it. Trial complexity and length would be significantly increased.

ANNEX E: THE 'INTERCEPTION CASE' MODEL

E1. This model was proposed by Lord Carlile and is based on material for the Privy Council review in 2007-08.

E2. Under this model, a category of intercept cases would be devised, where if in the course of an investigation it became clear that intercept material of real evidential value in the courtroom could be made available, the Attorney General or the Director of Public Prosecutions could be asked by the investigating agency to designate it an 'interception case'.

E3. The 'trigger point' for designating an investigation an 'interception case' would occur at some point after a criminal investigation had commenced (as defined by the Criminal Procedure and Investigations Act) but before the CPS considered specific charges. It would be desirable (to maximise the evidential material available to the prosecution and minimise potential Article 6 challenges at court) for 'designation' to take place as soon as possible after the criminal investigation had commenced.

E4. Examination, retention and review practice would depend on whether an investigation was designated:

- In a 'designated' investigation: examination, retention and review would follow Criminal Procedure and Investigations Act 1996 processes (or in the case of intelligence agencies their equivalents). Any material intercepted pre-designation that had been retained would remain non-admissible and would be subject to existing RIPA 'Preston' safeguards.

- In a 'non-designated' investigation: intercept product would remain non-admissible under the RIPA ban and agency practice would continue as now. The current RIPA 'Preston' safeguards would continue to apply.

E5. Charges would be brought and trials conducted as now.

E6. In order to promote transparency and accountability, the Interception Commissioner would be informed when an 'interception case' was initiated and of key developments. He would, either at the conclusion of each case or within his annual report, provide a narrative and assessment. This would not trespass on the judgments of the court in a given case but rather provide a further independent scrutiny of process and wider public accountability.

E7. The interception case boundary (or 'box') would be defined in legislation and comprise a number of 'filters'. So:

- It would be available (but not *required*) for a specific sub-set of serious offences for which interception is already permitted[11], for instance murder, attempted murder, conspiracy to cause explosions, drugs importation, money laundering, or serious fraud. Primary legislation would either specify the list of 'eligible' offences itself OR

[11] Under RIPA, interception is permitted: in the interests of national security; for preventing or detecting serious crime; for safeguarding the economic wellbeing of UK where it relates to national security; or giving effect to international mutual assistance. Serious crime is defined as (i) those crimes for which a person aged 21 or over with no previous convictions could expect to receive a jail sentence of three years or more and (ii) the conduct involves violence, results in substantial financial gain or is conducted by a large number of persons pursuing a common purpose.

provide for an order-making power to be exercised by the Secretary of State, subject to an affirmative resolution.

- 'Designation' would have to be 'in the interests of justice.' This would be defined in the primary legislation as: (i) there being reasonable grounds to believe that intercept evidence is likely in that case to be of material benefit at trial; and (ii) the disclosure issues arising in that case being manageable (i.e. not being likely to give rise to unfairness at trial). There is clearly a trade-off between these on the timing of when designation was sought.

- The Attorney General or the Director of Public Prosecution's agreement would need to be sought and secured to 'designate'. He or she would need to confirm that designation in a case was 'in the public interest.' The detailed basis for decision-making (i.e. underpinning the interests of justice criteria) would be set out in a Code of Practice.

E8. Depending on arrangements (to be decided) there would be pre-designation consideration based on national security or sensitive material, techniques, capabilities or relationships. For instance, this could form part of the 'interests of justice' consideration (e.g. if whether most or all 'telling' intercept was from sensitive sources and so was unlikely to be adduceable as evidence) or could be dealt with through a separate 'filter'.

E9. Legislation (along the lines of section 7 of the Justice and Security (NI) Act 2007) would make clear that no court may entertain proceedings for questioning (by way of judicial review or otherwise) any decision, or purported decision, by the Attorney General or the Director of Public Prosecutions in relation to designation other than on grounds of dishonesty, bad faith or other exceptional circumstances (in particular error of law or lack of jurisdiction).

E10. Non-designated trials would continue as now, under the RIPA ban.

E11. Complications arising in the case of 'multi-handed' trials where interception had been used and where the investigation against some suspects had been 'designated', but that into others had not (for instance, reflecting the prospective charges), would be addressed by holding separate trials for 'designated' and 'non designated' defendants.

ANNEX F: COSTS

F1. Fully-funded implementation of intercept as evidence would cost between £4.25 - £9.25bn[12] over the 20 year lifespan of the cost-benefit analysis. The table below breaks down costs under two scenarios - flat and high growth in volumes of communications:

Table F1: Cost under flat/ high growth:[13]

	Flat Growth £m	**High Growth £m**
Staffing	3,230	7,710
Systems	465	480
Accommodation	330	800
Agencies SUB-TOTAL	**4,025**	**8,990**
Additional interception technical costs	250	265
Interception-related TOTAL	**4,275**	**9,255**

Potential cost mitigations

F2: Testing was also undertaken to explore how far it might be possible to reduce the estimated costs by management and other action. A series of 'potential mitigations' were identified which, if possible to implement, would have a material impact on overall costs. They include:

- **Potential mitigation 1:** that by the final year of cost benefit analysis period emerging technologies mitigate staff examination and review costs by (i) 12.5% or (iii) 25%[14].

- **Potential mitigation 2:** use of existing technologies (e.g. 'click and drop' and 'predictive text') to support manual effort (typing time) in processing (gisting and summarising) intercept. There is no scope for it to do so with transcription.

- **Potential mitigation 3**: limiting retention post conviction to a fixed period of three years (unless an appeal is underway);

- **Potential mitigation 4**: limiting retention post investigation to a maximum period of three years. Risks comprise (i) appeals being subsequently sought successfully OR (ii) individuals subsequently being found to be criminals, post-deletion.

- **Potential mitigation 5**: business change is able to mitigate 20% of the additional staffing costs arising from additional 'gisting'; 'summarising' and 'transcription' under intercept as evidence.

F3. While all potential mitigations were tested, interception agencies doubt whether mitigations 2 and 5 would be possible.

[12] Net Present Value over 20 years, excluding criminal justice systems costs related increases/decreases in the number of prosecutions and convictions and rounded to nearest 5m.
[13] Net Present Value (NPV) – over the 20 year time span of the cost benefit analysis.
[14] 25% over 20 years – i.e. technological gain of around 1%pa – is illustrated in the tables

F4. The implications for net present value costs for intercept as evidence over the 20 years of the cost benefit analysis are set out below.

Table F2: Impact of mitigations on Flat Growth scenario[15]

Cost £m	**Flat Growth**	PM 1	PM 2	PM 3 & PM 4	PM 5	PM 1 to 5
Staffing	3,230	2,770	2,470	3,230	2,675	1,690
Systems	465	465	465	460	465	460
Accommodation	330	290	260	325	330	220
TOTAL	**4,025**	**3,525**	**3,195**	**4,015**	**3,470**	**2,370**

Table G3: Impact of mitigations on High Growth scenario[16]

Cost £m	**High Growth**	PM 1	PM 2	PM 3 & PM 4	PM 5	PM 1 to 5
Staffing	7,710	6,565	5,965	7,710	6,395	4,075
Systems	480	480	480	480	480	480
Accommodation	800	690	645	790	800	530
TOTAL	**8,990**	**7,735**	**7,090**	**8,980**	**7,675**	**5,085**

F5. Potential mitigations 3 and 4 (retention periods) have little possible impact, because storage space accounts for only a very small share of cost. This suggests, given the additional legal risk involved, they would be unlikely to be worth pursuing. Potential mitigations 1, 2 and 5 have much greater possible impact because they operate primarily on staffing, which accounts for the majority of additional cost. Combining them all generates a mitigation of around 40% of additional cost in Net Present Value terms – although the absolute costs remain high (£2.4 to £5.1bn).

[15] For the Straight Real Model, Net Present Value (NPV) – over the 20 year time span of the cost benefit analysis rounded to nearest 5m.
[16] ibid

ANNEX G: EMERGING TECHNOLOGIES

G1. At its outset, the review explored the scope for future technological change to reconcile the legal and operational requirements, by mitigating the impact of a legally viable approach such that it could be broadly affordable within existing agency funding.

Emerging Technologies

G2. Applying a Criminal Procedure and Investigations Act 1996 compliant approach would require voice interception being analysed in full, with the content being retained and 'gisted' or 'summarised' for later review. The result would be a requirement for large numbers of additional staff, with significant cost and feasibility implications. Scoping analysis conducted in the Privy Council Review assessed whether recent or future advances in electronic storage, transcription, translation and search might enable the (more or less) full automation of these processes. The key elements of this were:

- Full retention storage of intercept material: because this is a requirement for evidential regimes.

- Automated speech processing tools

- Effective searches of stored material: key word and other search techniques would then be used to identify potentially exculpatory material at the pre-trial review stage.

G3. These would not – even if legally and technically viable – obviate cost. However these tools could – if viable – make a major difference to the costs set out in the body of this report and practicalities of otherwise providing the staff required for a Criminal Procedure and Investigations Act 1996 compliant examination and review. The conclusions of the Privy Council Review, set out to Parliament[17], were that although the first of the three elements would be feasible (if costly), at least in the foreseeable future, the other two elements necessary would not be.

G4. Given the complexity and rapidly changing nature of capabilities in this field, this review subjected these technical findings to independent external validation. Having assessed a range of possible candidates, an independent consultancy was selected on the basis of relevant technical expertise and appropriate security clearances. This was supplemented with a further review by the Home Office Centre for Applied Science and Technology.

G5. Their conclusions are summarised in the table overleaf. These confirm the original finding that technology does not at present provide a feasible means of reconciling the legal and operational requirements. However, where emerging technology might reasonably be expected to contribute to potential cost mitigation, this would be fed into the assessment of advantage cost and risk.

[17] See Written Ministerial Statement by the then Home Secretary of 26 March 2010.

2010 VALIDATION OF CONCLUSIONS ON EMERGING TECHNOLOGIES

Area Assessed	Review Paper 'Full Retention' Storage and Technology-Enabled Review	Independent Consultancy	Centre for Applied Science and Technology (CAST)
'Full retention' storage of intercept material	The changing communications environment made it difficult to reach definite conclusions on the feasibility of full retention storage. However, the scoping work undertaken suggested that it would be **likely to be technically feasible, albeit costly**.	**Agree with the report conclusion** that full retention is feasible in a short period of time, but would be very costly.	The report's conclusions on full retention storage **are realistic and practicable**, assuming some filtering (of high volume material) is considered acceptable.
Automated speech processing tools	Although some automated speech processing tools do exist, accuracy falls off rapidly as audio quality declines to the level found in intercept material. There seems **little prospect of attaining the necessary accuracy and flexibility in the near future**.	Differ on some of the arguments and evidence but **agree that the conclusion of the report** is **'agreeable' and accurate**. There is a large amount of work ongoing in this field, but it does not seem likely that high levels of accuracy would be achieved in the near term. No transformational technologies are in the pipeline.	Conclusions on automatic analysis/search tools are **considered realistic**, although there is significantly more uncertainty around availability of improved capabilities in this area over the timescales being considered.
Effective searches of stored material	**Searching the resultant text is problematic**: the inability to define search terms sufficiently is likely to result in reviewers being swamped with 'false positives' and even sophisticated e-discovery programmes are unlikely to capture all relevant material.	Concludes that an effective and flexible search system of stored data, whilst difficult to produce, **is feasible in the foreseeable future**, but again at a considerable cost.	
Expected performance improvements and assessment of other technologies	Unlikely that searches of non-text material will develop sufficiently in next 5-10 years. Little prospect of development of transcription and translation to required standards in same period.	Assessment highlights developments in automatic speech recognition and searching, although **neither seems to suggest required levels of development in near future**. The assessment also suggests a range of alternative technologies[18] that could aid full retention review, which require further consideration, but do not on their own offer full mitigation of the burdens of full retention.	The horizon-scanning in the report is considered to be reasonable, although the assumptions on the rate of development of some automatic processing techniques are considered slightly optimistic.

[18] Such as; additional language models, out of bounds search terms, multi-speaker recognition and speech separation, stream processing, spoken term detection, speech to speech translation and speaker detection.

Further Review and Industry Survey

G6. A further technology review was conducted in 2013. The aim was to refresh the previous findings and to focus on voice transcription and translation capabilities in order to assess whether the shortfalls identified in 2010 had diminished sufficiently to meet evidential standards. The industry survey commissioned sought to draw out capability in very specific areas of challenge for an evidential regime, chiefly accuracy in intercept conditions where audio quality is poor.

G7. The results showed that whilst there are a number of voice transcription and translation technologies, of varying capabilities, the technology is not sufficiently advanced to meet the needs of an intercept as evidence regime. Where there are optimal conditions some technologies offered an accuracy rate exceeding 90%. But there was a dramatic decline across all technologies with changes in quality of conditions; this reflected operational reality.

G8. Where the emergence of new technologies could be expected to contribute to cost mitigation, by lessening the need for manual examination, notation and review, this will be fed in to a reassessment of advantage, cost and risk.

ANNEX H: APPROACH TO ESTIMATING BENEFITS

H1. Benefits (additional prosecutions and convictions) have been assessed on the following basis:

- The first stage was to estimate the 'maximum potential' impact that introducing intercept as evidence could have on successful prosecutions. The figure of one arrest per warrant for serious and organised crime was used as the highest estimate; this was scaled for terrorism prosecutions. The figures were combined to produce a maximum potential of additional convictions possible from an intercept as evidence regime;

- Second, this 'maximum potential' was adjusted (downwards) for various 'reducing factors', which would counter (to greater or lesser extent) this potential maximum uplift. These are set out in more detail below.

H2. The interception agencies and the Crown Prosecution Service have conducted a top down 'sense-check' of the resulting overall magnitudes.

H3. A variety of factors which could reduce the number of successful prosecutions were run to show a range of possible benefits outcomes:

- **Encryption:** Considered the amount of intercept that would be unreadable due to encryption and the impact on evidential usage of encrypted material being readable but too sensitive to be used.

- **Some interception targets would be innocent or there would still be insufficient evidence:** Even using intercept as evidence there will likely be cases where insufficient evidence was gathered or the interception target was found to be innocent.

- **Changes in target behaviour resulting from the disclosure of interception capabilities and modus operandi:** The introduction of intercept as evidence would inevitably generate greater awareness of interception techniques. Two ranges were developed for counter-terrorism and serious and organised crime, to take into account the nature of the activity involved and the awareness and ability amongst different target groups.

- **The need to avoid bringing charges, or if necessary to drop cases, in order to protect sensitive capabilities/relationships.** The introduction of intercept as evidence would necessitate more active forethought and case management as a criminal investigation developed, in order to try and avoid the possibility of sensitive capabilities or relationships being exposed (or potentially exposed) in court. While there would be potential mitigations to revelation of sensitivities (including PII) there would be cases where these were insufficient and the only option would be to withdraw prosecutions and convictions.

- **Problems in proving attribution or authentication:** Key factors would include the likely share of voice and non-voice-based communications.

H4. Plausible numbers of unsuccessful convictions were applied to each of these factors to estimate credible future benefits. Most of the factors above remained constant through the life-span of the cost benefit analysis. There were two factors that were identified as likely to change:

- **Greater Awareness:** The awareness of interception techniques and capabilities is likely to grow as evidence derived from intercept is used more widely.

- **Attribution/authentication**: The number of cases lost due to attribution and authentication issues would be likely to be higher earlier rather than later in the cost benefit analysis lifespan. To model this, levels of prosecutions and convictions withdrawn due to attribution/ authentication issues were doubled at the introduction of intercept as evidence and then gradually reduced to a steady constant.

ISBN 978-1-4741-1341-0