



Intercept as Evidence

A Report



Intercept as Evidence

A Report

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

December 2009

© Crown Copyright 2009

The text in this document (excluding the Royal Arms and other departmental or agency logos) may be reproduced free of charge in any format or medium providing it is reproduced accurately and not used in a misleading context. The material must be acknowledged as Crown copyright and the title of the document specified.

Where we have identified any third party copyright material you will need to obtain permission from the copyright holders concerned.

For any other use of this material please contact the Office of Public Sector Information, Information Policy Team, Kew, Richmond, Surrey TW9 4DU
or e-mail: licensing@opsi.gov.uk.

ISBN: 9780101776028

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

ID 2338743 12/09 981 19585

Printed on paper containing 75% recycled fibre content minimum.

CONTENTS

Foreword	page 4
Introduction	page 5
The work programme and model	page 6
Main findings	page 7
Evidential impact	
Legal viability	
Operational viability	
Costs	
International comparisons	
The feasibility of reversion to the current regime	
Conclusion and next steps	page 11
Annexes	
A The operational requirements	page 12
B The work programme	page 14
C The intercept as evidence model	page 18

FOREWORD

The Government has no higher duty than to protect the public. A critical tool in this is the warranted interception of communications that allows law enforcement and intelligence agencies to gather intelligence about terrorists and other serious criminals who seek to do us harm. Since I became Home Secretary, I have seen at first hand the value of interception in preventing terrorism and serious crime.

It has been, and remains, the Government's objective to build on this success by also enabling intercept material to be used as evidence in criminal trials, so that more of the guilty are prosecuted and convicted. That is why in February 2008 the Government accepted the recommendations of the Privy Council review and set in train the necessary implementation process. At the same time the Privy Council review underlined the overriding importance of continuing to meet the operational requirements necessary for public protection and national security. The importance of these operational requirements also led the Government to establish the cross party Advisory Group of Privy Counsellors to ensure that they were respected.

This report sets out the key findings and conclusions of this work. These confirm the potential gains from a workable scheme for intercept as evidence and that, while requiring significant additional funding, the model developed would be broadly consistent with the operational requirements identified. However, it is also the case that the model would not be legally viable, in terms of ensuring continued fairness at trial. The result would not only be potential miscarriages of justice and more expensive and complex trials but also more of the guilty walking free.

These findings are such that no responsible Government could proceed with implementation on this basis. The Advisory Group concurs with this overall judgement. At the same time, both the Government and the Advisory Group believe that the potential gains from intercept as evidence justify further work, in order to establish whether the problems identified are capable of being resolved. We will take this work forward urgently and report back to Parliament.

The issues involved are complex and difficult, and addressing them commensurately challenging. But the importance of our interception capabilities to national security and public protection means that there can be no short cuts.

A handwritten signature in black ink, reading "Alan Johnson". The signature is written in a cursive style with a large, sweeping initial 'A' and a long horizontal stroke above the 'J'.

Alan Johnson

Introduction

1. The lawful interception of communications¹ plays a critical role in tackling serious crime and protecting the British public. Almost all of the highest priority counter-terrorist operations and many other serious crime investigations involve the use of intercept. The strict legal safeguards that govern interception are set out in the Regulation of Investigatory Powers Act 2000 (RIPA) to ensure that it is used proportionately, under the specific authority of a Secretary of State, and that people's privacy is respected.

2. Intercept material obtained under a RIPA warrant cannot currently be used as evidence in criminal trials. It has been, and remains, the Government's objective to find a way to make this possible. In February 2008, the Prime Minister accepted the findings of a Privy Council review, chaired by Sir John Chilcot, which recommended that intercept should be admissible as evidence subject to meeting nine operational requirements, which the review judged to be necessary to protect the public and national security². They are set out in **Annex A**, with a brief explanation, and their significance is summarised below.

The importance of the operational requirements

Sensitive intercept material, techniques and capabilities must be protected to avoid terrorists and other serious criminals evading detection and frustrating the investigation of their activities. Most targets have a rudimentary understanding of interception capabilities based on observation of police work and court proceedings, but it will be very imprecise. If terrorists and other criminals develop a more accurate understanding of the techniques and capabilities deployed against them, the task of protecting the public and national security will be considerably harder (operational requirements 1 to 3 and 9).

The interception agencies are able to respond to rapidly evolving operational demands and new information by constantly reprioritising between different operations. Continued discretion over retention, examination and transcription practice is essential to this. It ensures that the scarce resources – money and highly-trained staff – can be used to best effect (operational requirements 4 and 5).

Tactical interception provides real-time intelligence on terrorists and criminals and facilitates the collection of evidence so that their plans can be disrupted and actions frustrated. Strategic interception, often over a longer period of time, is essential to our understanding of the terrorist and criminal threat facing the UK (operational requirements 6 and 7).

¹A variety of related techniques giving legally authorised access to communications ranging from letters and calls between two fixed telephones to complex multi-media internet sessions.

² Privy Council Review of Intercept as Evidence Report to the Prime Minister and the Home Secretary, 30 January 2008, Cm 7324

The close co-operation between law enforcement and intelligence agencies that characterises the UK's use of interception brings extensive benefits. It avoids duplication of effort, ensures effective information sharing and means that best practice and sensitive interception techniques can be deployed effectively (operational requirement 8).

3. The Government therefore commissioned a programme of work to implement the recommendations of the Privy Council review in a way which met the operational requirements it set. The programme was led by the Office for Security and Counter Terrorism in the Home Office and involved the intercepting agencies, investigators, prosecuting authorities and a range of senior independent legal practitioners. Building on the original Privy Council review, an Advisory Group of Privy Counsellors³ was also set up to advise the Team and ensure that the operational requirements were met.

4. This report summarises the findings and conclusions of the work programme. The sensitivities involved mean that the full weight of supporting evidence cannot be made public. This has been made available to Ministers and to the Advisory Group.

The Work Programme and Model

5. The Implementation Team carried out a programme of work, which comprised 'design', 'build' and 'test' phases of activity, reflecting the approach recommended by the Privy Council review. The programme was subject to rigorous oversight – by senior officials, Ministers and the Advisory Group of Privy Counsellors – to ensure the integrity of the process and its conclusions. The work programme and governance structure are summarised in **Annex B**.

6. The model developed was based on an approach, known as "Public Interest Immunity Plus", which the Privy Council review concluded was the most likely to be legally viable of those they had considered. The model is summarised in **Annex C**. The Privy Council review also made clear the need for consistency with the operational requirements it had set out, among which continued discretion over retention, examination and review of intercept material is central.

³ Comprised of the Rt. Hon. Sir John Chilcot, the Rt. Hon. Lord Archer of Sandwell, the Rt. Hon. Sir Alan Beith MP, and the Rt. Hon. Michael Howard QC MP

Main Findings

7. The project looked at the potential evidential benefits of an intercept as evidence regime; and whether the model developed to deliver them could both be legally viable and meet the Privy Council review's operational requirements. The main findings are as follows:

I. Evidential Impact

8. Evidence from intercept material is likely to support some prosecutions relating to a range of serious criminal offences. Practical testing in the final phase of the work programme demonstrated that significant amounts of incriminating material would be generated although it would be unlikely to secure a conviction on its own. This benefit needs to be set against the factors outlined in paragraphs 10 and 14 below.

9. Context and the use of veiled and opaque language could be explained by expert witnesses although defences would often challenge attribution (i.e. who the speaker or author of the intercepted material was) and the reliability of interception systems. This would be likely to make trials more complex as a result.

II. Legal Viability

10. To realise these evidential benefits, the intercept as evidence model needs to be legally viable. The unanimous legal advice, including from independent Counsel, is that testing has shown that the model developed in this work programme would not be legally viable.

11. In order to comply with the fourth and fifth operational requirements (ongoing agency discretion over the retention, examination and transcription of intercept material), the model does not require the retention of all intercepted material. For the same reason, although the model incorporates a degree of judicial oversight, it does not give judicial control over the intercepting agencies' retention, examination and review processes.

12. The legal difficulties with such a model arise primarily because, in practice, full retention (or judicial control over what may be discarded) is likely to be essential to ensure fair trials under an intercept as evidence regime. A recent Strasbourg decision⁴ has confirmed this conclusion. The key point concerns the non-retention of intercept material within an evidential regime, without a robust system of judicial oversight.

⁴ Natunen v Finland 31 March 2009. Final version on ECHR portal 30 June 2009

13. This extensive retention requirement within evidential intercept regimes arises because the Crown could use intercepted material to make its case. Accordingly, to achieve equality of arms between the prosecution and the defence, the Crown would need, as with any other type of evidence, to accept the burden of finding and keeping any intercept material that casts doubt on its interpretation of the evidence or supports a defence case. In practice, the full retention of all intercepted material is necessary to ensure equality of arms in an evidential regime.

14. Because the testing phase confirms that the model does not meet the necessary fair trial (Article 6 ECHR and domestic law) requirements, trial judges would be likely to exclude intercept evidence or halt the proceedings in the majority of cases – particularly in the sorts of complex trials regarding terrorism or other serious criminal offences. There would be a significant risk in cases even where the prosecution was not itself seeking to use intercept material. Where intercept material was not excluded or the trial halted, legitimate defence challenges based on requests for disclosure or on admissibility and attribution would add significantly to trial complexity and length.

15. The current RIPA regime meets the equality of arms requirements of Article 6 precisely because it is not evidential: neither the prosecution nor the defence can draw on intercepted material in evidence. This approach has been approved by both UK courts and the European Court of Human Rights.

III. Operational Viability

16. The model was tested against the nine operational requirements identified by the Privy Council review:

- *Operational requirements 1 to 3: intercepting agencies should have the final say over the use of intercept material in legal proceedings to protect sensitive techniques and capabilities.* The proposed approach, while complex and resource-intensive, would probably meet these requirements, although in order to protect sensitive information, techniques and capabilities, some cases would not reach trial. Usage over time in court would, however, make some exposure of sensitivities inevitable.
- *Operational requirements 4 to 5: agencies should have continued discretion over retention, examination and transcription of intercept material.* An evidential regime would impose additional burdens. Without significant additional funding, this would cause a substantial reduction in the number of interception operations that agencies could undertake.

- *Operational requirements 6 to 8: agencies should be able to maintain their real-time tactical and long-term strategic capabilities; day to day co-operation between law enforcement and intelligence agencies should not be affected.* It should be possible to meet these requirements but significant additional funding and changes to current operational practice would be required – reflecting the more stringent requirements of an evidential regime. Risks to current capabilities would remain, in particular to co-operation between law enforcement and intelligence agencies.

The benefits of inter-agency co-operation – a case study

In 2008 British members of an overseas-based criminal group conspired to import and distribute regular consignments of Class A drugs into the UK and to launder the proceeds.

Interception began at an early stage, facilitated by the tasking of the intelligence agencies, and proved crucial in frustrating the conspiracy.

Intelligence agency support for law enforcement was critical in enabling the scale and modus operandi of the conspiracy to be identified at an early point and for the investigation to be guided effectively as the conspiracy developed.

Agency support also identified the location of a planned drugs importation, directly leading to multi-kilogramme drug seizures, multi-million pound cash seizures arrests at the scene and subsequent convictions. Steps are in hand to confiscate their criminal proceeds.

- *Operational requirement 9: the model should, prevent successful speculative 'fishing expeditions' by the defence.* Problems would arise but should be manageable, with judges applying current trial guidelines appropriately. Nevertheless, as explained above, the model would also result in legitimate defence challenges, increasing trial lengths.

17. The Privy Council review also emphasised the importance of being able to protect the interests of Communication Service Providers (CSPs - the companies that provide fixed and mobile telephone, internet-based or other communications services) and international partners. The Implementation Team consulted extensively but significant concerns remain. The vast majority of CSPs consulted believed that the model would not be capable of protecting their staff or involvement in supporting lawful interception. This leaves a significant risk that proceeding with implementation would jeopardise the valuable support provided by CSPs in combating terrorism and other serious crime.

IV. Costs

18. The costs of implementing intercept as evidence would be very significant. They would include:

- Initial set-up costs (e.g. enhancing interception systems to the appropriate evidential standard).
- Increased ongoing running costs (e.g. additional staff required to monitor, review and transcribe intercept).
- The costs of operating the systems certification and judicial oversight regimes and gathering of supporting evidence to facilitate the use of intercept in court.

19. In addition, there could be significant costs for the criminal justice system, reflecting possible impacts of greater trial complexity on courts and legal aid.

V. International Comparisons

20. Other countries make use of intercept as evidence, but the original Privy Council review concluded that different legal and operational contexts made their experience of limited relevance in assisting implementation in the UK. Overseas experience does indicate that the operational burdens for the intercepting agencies are considerable. Fewer investigations can be supported and the value of intercept as an intelligence tool is significantly reduced.

21. None of the countries examined in the course of this work programme or by the Privy Council review has developed the degree of inter-agency co-operation enjoyed by the UK; overseas law enforcement agencies generally have more limited access to sophisticated intelligence agency interception techniques than is the case here. The combination of the ECHR, as reflected domestically in the Criminal Procedure and Investigations Act 1996, and our adversarial court process makes disclosure obligations more onerous in this country than some others. All these factors significantly increase the risk that the evidential use of intercept would compromise sensitive techniques or necessitate cases being dropped in order to avoid doing so. The result could be to undermine investigations which currently lead to successful prosecutions.

VI. The Feasibility of Reversion to the Current Regime

22. The Privy Council review made it clear that after introducing an intercept as evidence regime the Government should retain the ability to modify the regime or re-impose the present ban in the event that the operational requirements were subsequently jeopardised. However, independent legal advice is that a full return to the present position could not be guaranteed. This is because there are likely to be some subsequent trials in which a reimposed ban might be assessed by the court as not being justified (for instance where the intercept concerned was non-sensitive). By creating a precedent, this would in turn gradually undermine the re-imposed ban more widely.

Conclusion and Next Steps

23. The collective view of the Departments, intercepting agencies and prosecution authorities engaged in the work programme is that despite best efforts to design, build and test the model, it does not provide a viable basis for implementation, without breaching the operational requirements set out by the Privy Council review. The central issue remains the need to reconcile:

- The implications for retention, examination and review of intercept material if trials under an evidential regime are to remain fair; and
- Continued agency discretion over these matters if current investigative and intelligence capabilities are to be maintained.

24. Implementation on the basis of the “PII Plus model” proposed by the Privy Council review would weaken and not enhance our ability to protect the public and to identify and bring the guilty to justice.

25. The Government nevertheless remains committed to the principle of introducing the use of intercept as evidence, if this is possible while meeting the necessary operational requirements. So it welcomes the suggestion by the Advisory Group of Privy Counsellors to pursue three further areas of work to try to identify a way forward. Beyond the scope of the original programme, these would explore the implications for legal and operational viability of:

- Further enhancing the judicial oversight available.
- Full retention of intercept material alongside alternative review requirements.
- Advances in technology, which might make full retention and review more manageable.

26. This work will be led by the Implementation Team in close co-operation with the intercepting agencies and the prosecuting authorities. The results will be reported to Parliament before the Easter recess.

ANNEX A: THE OPERATIONAL REQUIREMENTS

This annex sets out the key operational requirements established in the Privy Council review alongside the application and comment subsequently agreed by the Advisory Group of Privy Counsellors to facilitate the work programme.

OPERATIONAL REQUIREMENT	APPLICATION AND COMMENT
<p>1. The intercepting agency shall decide whether a prosecution involving their intercepted material shall proceed.</p>	<p>The decision whether to prosecute a case or not remains with the relevant prosecuting authority.</p> <p>The decision whether to provide intercept evidence rests with the intercepting agency.</p> <p>Clearly the availability or otherwise of intercept will impact on the relevant prosecuting authority's assessment of case credibility and decision on whether to proceed or not.</p> <p>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.</p> <p>"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.</p>
<p>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.</p>	<p>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.</p> <p>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".</p>
<p>3. 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 & techniques at risk.</p>	<p>Any disclosure of intercept acquired through 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.</p>

<p>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).</p>	<p>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.</p>
<p>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).</p>	<p>The agency cannot be required to alter its operational monitoring or transcription requirements.</p> <p>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).</p>
<p>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.</p>	<p>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.</p>
<p>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.</p>	<p>Existing law enforcement agency capabilities to undertake and ability to retain and protect long-term strategic intelligence will not be impaired.</p> <p>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.</p>
<p>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.</p>	<p>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.</p> <p>However, any such product would be subject to the same Agency veto safeguards as set out in operational requirements 1, 2 and 3, above.</p>
<p>9. 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.</p>	<p>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 CPIA processes). This includes those dealt with under the PII Plus processes (e.g. operational requirements 1 to 3 above).</p>

ANNEX B: THE WORK PROGRAMME

The implementation work programme directly reflected the approach recommended by the Privy Council review and comprised 'design', 'build', and 'test' phases of activity.

Model design (Phase 1)

B2. This phase involved development of an intercept as evidence regime, starting from the 'PII Plus' model, recommended by the Privy Council review, by:

- Developing the model consistent with the operational requirements, identifying practical approaches to protecting sensitive material, techniques and capabilities and reconciling agency flexibility over examination, retention and review of intercept material with the requirements of fair trials.
- Addressing other implementation issues, notably the potential implications for: civil proceedings (ensuring that the use of intercept in criminal trials did not give rise to security risks in associated civil cases); current interception systems (the practicalities and cost of upgrading as necessary for evidential use); and reversion to the present regime should subsequent developments make that necessary. Work also started on a framework for assessing potential costs.
- Examining wider implications – for instance for the wider criminal justice system.

B3. The model would require changes not only to the Regulation of Investigatory Powers Act 2000 (RIPA) but also to other existing legislation, such as the Criminal Procedure and Investigations Act 1996 (CPIA), with the CPIA's 'relevancy' test and other features being amended. It would also mean significant changes to how the interception agencies operate – notably through the introduction of detailed statutory codes of practice and of advisory oversight of interception operations by retired judges, in a new role of 'oversight commissioners'.

B4. The first phase of work was completed in November 2008.

Model build (Phase 2)

B5. This phase considered the consequences of the model in more detail, turning the policy approaches developed during the first phase of work into the relevant operational guidance and legal framework. This involved:

- Preparing operational policies and guidance for those agencies undertaking a “live test” of the intercept as evidence model and the illustrative legislation needed in order to simulate related trial processes in the final phase of work.
- Investigators, interception agencies and prosecuting authorities undertaking desktop scenarios against a representative sample of previous operations. This involved over a hundred operational staff.
- Work on wider implementation – importantly, on the implications for interception systems and on developing the framework for assessing the potential costs.

B6. This phase ran from December 2008 to the end of February 2009.

Model test (Phase 3)

B7. This phase assessed whether the model met the necessary fair trial and operational requirements, by:

- Undertaking live tests of interception practice led by three law enforcement agencies, and supported by two other interception agencies. Each took an investigation and, in parallel, tested the practicalities of an intercept as evidence regime based on the policies and guidance developed in phases 1 and 2 of the project. The focus was on: establishing the evidential impact of intercept material; legal viability, in particular the ability of agencies to operate consistent with the requirements of ensuring fair trials; and consistency with the operational requirements identified by the Privy Council review.
- Assessing the ability of agencies and prosecuting authorities to protect sensitive material, by defining those sensitivities and applying the necessary safeguards in practice.
- Simulating key trial processes to examine how the fair trial issues identified in the live tests would play out in court. The case involved illustrative charges of money laundering and conspiracy to supply drugs and was chosen because it was representative of large

operations in which intercept typically plays an integral part. The trial process included:

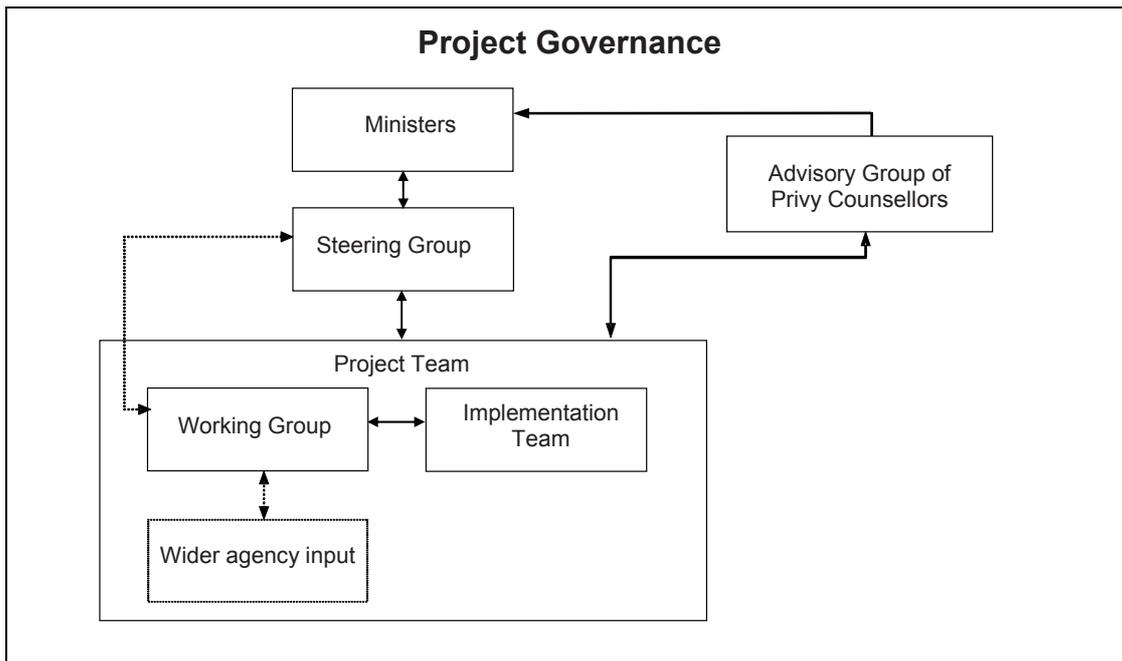
- The prosecution opening case and the application for PII in response to a defence disclosure request for sensitive material.
 - A defence abuse of process argument that the trial was unfair.
 - A closed admissibility hearing designed to protect the source of sensitive evidential intercept.
 - Presentation of intercept product in evidence, supported by agency experts and witnesses.
- Drawing conclusions on the implications for interception systems and the likely costs, given the findings across the work programme as a whole.

B8. Senior independent legal practitioners who participated in the live tests and in the trial simulation included a retired High Court judge, a retired Crown Court judge, three QCs, and an experienced SOCA/HMRC prosecutor. Formal legal advice was also obtained from external Counsel: a senior criminal law QC and Treasury Counsel specialising in European human rights law. The Interception Commissioner, Sir Paul Kennedy, was made aware of and was content with the conduct of live tests and trial simulation. He referred to this work in his annual report.

B9. Throughout the work programme, and in particular during the second and third phases, the Implementation Team consulted communication service providers and other interested parties. It also sought to identify lessons from experience overseas.

Programme governance

B10. In recognition of the complexity and importance of the subject matter, the project was subject to rigorous governance, summarised below:



B11. A **Steering Group**⁵ of senior officials provided oversight, direction and management of the project.

B12. The **Advisory Group of Privy Counsellors** provided advice to the Implementation Team and Ministers, to ensure that the key objectives of safeguarding intelligence capability and protecting the public were not harmed as a scheme was developed.

B13. The **Project Team** comprised a full-time **Implementation Team**, based in the Office for Security and Counter Terrorism within the Home Office, responsible for delivering the work programme and a **Working Group** of interception and prosecuting agency stakeholders supporting the Implementation Team and acting as points of contact to identify and facilitate the input of wider expertise.

B14. In total the staffing and other resource costs of undertaking the review are estimated at £2.5m, mostly staff costs in departments and agencies. The demands of the final, testing, phase of the project necessitated the reprioritisation of some live operations. Over the course of the project several hundred people were involved, peaking at some 50 Full Time Equivalents, during the final phase of work.

⁵ Representing the Attorney General's Office, Association of Chief Police Officers, Cabinet Office, Crown Prosecution Service, Foreign & Commonwealth Office, Government Communications Headquarters, Her Majesty's Revenue & Customs, Home Office, Metropolitan Police, Ministry of Justice, Northern Ireland Office, Office for Criminal Justice Reform, Police Service of Northern Ireland, Revenue & Customs Prosecution Office, Scotland Office, Secret Intelligence Service, Security Service, Scotland Office, Serious Organised Crime Agency, and the Strathclyde Police.

ANNEX C: THE INTERCEPT AS EVIDENCE MODEL

Sections 17 and 18 of the Regulation of Investigatory Powers Act 2000 (RIPA) would no longer apply for criminal proceedings. The relevant Secretary of State would continue to sign warrants as now. All material from intercepted communications would be potentially admissible as evidence.

C2. Intercepting agencies would continue to have discretion over monitoring, retention and transcription practices. Material assessed by the agencies at the time of examination as being potentially exculpatory (i.e. which either supports the defence case or undermines that of the prosecution) would be retained. To help ensure the fairness of trials and protect individuals' right to privacy, the model would require:

- Amendment of the Criminal Procedure and Investigations Act 1996 (CPIA), so that intercept material would continue to be exempt from its usual retention and review requirements. Intercept would only be retained if it was assessed at the time to be exculpatory, following which it would be disclosed before trial in the normal manner. This is intended to help ensure consistency with the operational requirements.
- A statutory code of practice, with general and case-specific operating guidance to set out intercepting agencies' responsibilities with respect to the examination, retention and review of intercept and to govern their application.
- Oversight of specific interception operations by retired judges to advise agencies on their retention practices in order to help them to identify exculpatory material and assure the courts that guidance was being adhered to. Their advice would not be mandatory but they would provide a report on interception practice in each case to the relevant trial judge.

C3. In order to protect sensitive material, agencies would have the final say over the use of their intercept material as evidence. However, the Crown Prosecution Service (or other prosecuting agencies) would, as now, retain control of the charges brought and the case as a whole.

C4. Closed admissibility hearings similar to existing Public Interest Immunity sessions would be used to address any defence challenge to the use of intercepted material where there could be a risk of disclosing sensitive material, techniques or relationships. The defendant's interests would be

represented by a Special Advocate. All matters going to evidential weight would continue to be for the jury in open court.

C5. All retained intercept material would be reviewed and, if relevant, would be disclosable to the defence. Where doing so would jeopardise sensitive material or techniques the prosecution would apply for PII. If the trial judge refused to grant PII, the prosecution would need to consider whether the case against the relevant defendant could be put a different way, so that the material in question was no longer at risk of being revealed (e.g. by dropping charges) and if not, the case as a whole would have to be dropped.

C6. To reduce the need for closed admissibility hearings and to minimise calls on agency and Communication Service Provider staff time in court, a statutory presumption would support the admissibility of intercept material, based on systems being accredited to approved standards of certification and testing.



information & publishing solutions

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

The Parliamentary Bookshop

12 Bridge Street, Parliament Square,

London SW1A 2JX

Telephone orders/ General enquiries: 020 7219 3890

Fax orders: 020 7219 3866

Email: bookshop@parliament.uk

Internet: <http://www.bookshop.parliament.uk>

TSO@Blackwell and other Accredited Agents

Customers can also order publications from

TSO Ireland

16 Arthur Street, Belfast BT1 4GD

028 9023 8451 Fax 028 9023 5401

ISBN 978-0-10-177602-8



9 780101 776028