The Use of Intercept Evidence in Terrorism Cases

Standard Note: SN/HA/5249
Last updated: 24 November 2011
Author: Alexander Horne
Section Home Affairs Section

This note provides background information about the prohibition on using intercept evidence in terrorism trials. Subject to a limited number of exceptions, evidence from intercepted communications or any related communications data is inadmissible in legal proceedings under provisions currently set out in section 17 of the *Regulation of Investigatory Powers Act 2000.* It is important to note that the bar on intercept extends beyond terrorism cases (concerns have been expressed in respect of coroner's inquests for example). However, this note only focuses on the use of intercept material in counter-terrorism proceedings.

Following the introduction of the *Prevention of Terrorism Act 2005*, which introduced the controversial power to make 'control orders' against terror suspects (for more on this see Control Orders and the Prevention of Terrorism Act 2005), and moves by the Labour Government to introduce extended periods of pre-charge detention, pressure has been brought to bear, by human rights NGOs and others, to find ways to allow intercept evidence to be used in criminal trials, to facilitate the prosecution of terror suspects.

The Government and its former Independent Reviewer of Terrorism Legislation, Lord Carlile QC, have never accepted that allowing intercept evidence would act as a "silver bullet" that would end the control order regime. Nonetheless, the Labour Government agreed to set up a Privy Councillor Review, led by Sir John Chilcot, to consider whether it would be feasible to make intercept evidence available in criminal trials. The Review first reported in February 2008. Following a series of updates, in December 2009, the Home Office concluded that the reports they had received were such that "no responsible government" could proceed with implementing the introduction of intercept evidence on the basis of the proposed model. The then Home Secretary, Alan Johnson, said: "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." The Labour Government did not entirely dismiss the idea of using intercept evidence and its advisory group was asked to explore other avenues to allow evidence to be admitted.

The Coalition Government has indicated that it is still pursuing this policy.

Contents

1 Background

1.1 *The Regulation of Investigatory Powers Act 2000 (RIPA)*

The *Regulation of Investigatory Powers Act 2000* permits specified intelligence and law enforcement agencies to intercept all forms of communications (by post as well as electronically) on the authority of a warrant given by the Secretary of State.[1] A warrant can be given for any of four purposes

- In the interests of national security
- For the purpose of preventing or detecting serious crime
- For the purpose of safeguarding the economic well-being of the United Kingdom.
- For the purpose (in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant for the purpose of preventing or detecting serious crime) of giving effect to the provisions of any international mutual assistance agreement.[2]

In Scotland, warrants for the purpose of preventing and detecting serious crime are given by Ministers in the Scottish Executive. Before giving a warrant, the Secretary of State must be satisfied that interception is necessary to obtain the information required; that the information could not reasonably be obtained by other means; and the interception is *proportionate* to what it seeks to achieve.[3] Warrants last for three or six months[4] depending on purpose, but can be renewed by the Secretary of State.

The activities and decisions of the Secretary of State, the Scottish Ministers and the intercepting agencies are overseen by the Interception of Communications Commissioner (currently Sir Paul Kennedy, a retired senior judge appointed for the purpose by the Prime Minister). The Commissioner has access to all relevant documents and material; all persons involved in interception are required by law to cooperate fully with him. He reports at least annually[5] to the Prime Minister, and these reports are published. An Investigatory Powers Tribunal[6] exists which considers complaints from the public about interception, and can order appropriate remedies.[7]

Subject to a limited number of exceptions, evidence from intercepted communications or any related communications data is inadmissible in legal proceedings under provisions currently set out in section 17 of the *Regulation of Investigatory Powers Act 2000.*[8] A similar prohibition

---

[1] One exception exist insofar as a senior official may issue a warrant in the absence of the Secretary of State in (a) a case of urgency (although the Secretary of State is still obliged to expressly authorise the warrant under s 7(2)(a) or (b) where the warrant is sought for the purposes of helping a foreign state under the terms of a mutual legal assistance agreement, so long as the suspect is outside the UK or the interception will take place only in relation to premises outside the UK (s 7(2)(b))

[2] Section 5(3)(a)-(d)

[3] Section 5(2)(b)

[4] Section 9

[5] Section 58(4)

[6] See: http://www.ipt-uk.com/default.asp?sectionID=8&chapter=2

[7] Privy Council Review of Intercept Evidence, January 2008, Cm7324, paras 17-19

[8] See for example, *Archbold*, Sweet and Maxwell, 2009, paras 25-367-25-381

was previously set out in section 9 of the *Interception of Communications Act 1985*, which was repealed by the 2000 Act.

Section 17 of the 2000 Act provides:

> 17 Exclusion of matters from legal proceedings (1) Subject to section 18, no evidence shall be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings which (in any manner)—
>
> (a) discloses, in circumstances from which its origin in anything falling within subsection (2) may be inferred, any of the contents of an intercepted communication or any related communications data; or
>
> (b) tends (apart from any such disclosure) to suggest that anything falling within subsection (2) has or may have occurred or be going to occur.
>
> (2) The following fall within this subsection—
>
> (a) conduct by a person falling within subsection (3) that was or would be an offence under section 1(1) or (2) of this Act or under section 1 of the [1985 c. 56.] Interception of Communications Act 1985;
>
> (b) a breach by the Secretary of State of his duty under section 1(4) of this Act;
>
> (c) the issue of an interception warrant or of a warrant under the [1985 c. 56.] Interception of Communications Act 1985;
>
> (d) the making of an application by any person for an interception warrant, or for a warrant under that Act;
>
> (e) the imposition of any requirement on any person to provide assistance with giving effect to an interception warrant.
>
> (3) The persons referred to in subsection (2)(a) are—
>
> (a) any person to whom a warrant under this Chapter may be addressed;
>
> (b) any person holding office under the Crown;
>
> (c) any member of the National Criminal Intelligence Service;
>
> (d) any member of the National Crime Squad;
>
> (e) any person employed by or for the purposes of a police force;
>
> (f) any person providing a postal service or employed for the purposes of any business of providing such a service; and
>
> (g) any person providing a public telecommunications service or employed for the purposes of any business of providing such a service.
>
> (4) In this section “intercepted communication” means any communication intercepted in the course of its transmission by means of a postal service or telecommunication system.

The prohibition on evidential use applies to material intercepted under an interception warrant or obtained unlawfully. It does not apply to interception which has lawful authority by virtue of the fact that both parties consent, or one party consents and a directed surveillance

authorisation is in place or it takes place under lawful business practice regulations. Accordingly, such communications are admissible in evidence (and disclosable). No equivalent prohibition applies to the evidential use of material obtained through surveillance, including eavesdropping[9], covert closed-circuit television, observations made by covert surveillance officers[10] and telephone conversations recorded by a hidden microphone not connected to the telephone. Moreover, it does not apply to material intercepted in a foreign country under that country's law. In all of these cases the material may be adduced as evidence, and is subject to the same disclosure rules as any other relevant material.[11]

As mentioned above, there are also some exemptions in relation to the ban (contained in section 18 of the Act). Many of these relate to proceedings where intelligence intercept material may be adduced, but where it is not provided to the suspect (for example 'control order' hearings, hearings before the Special Immigration Appeals Commission and the Proscribed Organisations Appeal Commission, etc.) In such circumstances a security cleared special advocate may be appointed to represent the interests of a suspect (for more on this see: Control Orders and the Prevention of Terrorism Act 2005).

1.1 A move to relaxing the ban on intercept?

The issue of whether to permit the disclosure and use of intercept evidence is not a new one. Between 1995 and 2008, there were seven reports to Ministers on the issue of intercept evidence.[12] Following the introduction of the *Prevention of Terrorism Act 2005*, which introduced the controversial power to make 'control orders' against terror suspects and (unsuccessful) government moves to try to extend the pre-charge detention of terrorist suspects (first to 90 and then to 42 days), pressure has been brought to bear, by human rights NGOs and others, to find ways to allow intercept evidence to be used in criminal trials, to facilitate the prosecution of terror suspects. In September 2006, it was reported that the then Director of Public Prosecutions, Ken MacDonald QC and the then Attorney General, Lord Goldsmith QC, were in favour of finding a way to lift the ban.[13]

The Government and its Independent Reviewer of Terrorism Legislation, Lord Carlile QC, have never accepted that allowing intercept evidence would act as a "silver bullet" that would end the control order regime. Nonetheless, on 2 February 2006, Charles Clark, then Home Secretary, made an oral statement about the renewal of the *Prevention of Terrorism Act 2005*. In it, he said the Government was seeking to find a legal model that would provide the necessary safeguards to allow intercept material to be used as evidence.[14]

On 28 February 2006, the then Assistant Commissioner of the Metropolitan Police, Andy Hayman, gave oral evidence to the Home Affairs Select Committee in connection with the Committee's inquiry into terrorism detention powers. In the course of his evidence, Assistant Commissioner Hayman noted that his view, and those of the Association of Chief Police Officers (ACPO), on the use of intercept evidence in court had changed over time. In particular, he said that while he originally had concerns that use of such evidence would

---

[9] For examples of admissible evidence from bugs see *R v Allsop* and others [2005] EWCA Crim 703; *R v E* [2004] EWCA Crim 1243

[10] Intelligence and Security Committee, Annual Report 2006-7, January 2008, Cm 7299, p 32, see also *R v Rosenberg* [2006] EWCA Crim 6

[11] Privy Council Review of Intercept Evidence, January 2008, Cm7324, para 22

[12] Privy Council Review of Intercept Evidence, January 2008, Cm7324, para 11

[13] *The Guardian*, "DPP backs Attorney's call to admit phone-tap evidence in court, 22 September 2006"

[14] HC Deb, 2 February 2006 c479

disclose methodology, he had concluded that that argument was "well and truly worn out". He added that:

> I think I am moving, as I know ACPO is, to a conclusion that in a selected number of cases, not just for terrorism but also for serious crime, it would be useful. I think also it does make us look a little bit foolish that everywhere else in the world is using it to good effect.[15]

In October 2006, the human rights and law reform NGO, JUSTICE published a report entitled *Intercept Evidence: Lifting the Ban.* It noted that:

> The report details how prosecutors in Australia, Canada, New Zealand, South Africa and the United States regularly use intercept evidence in prosecuting serious organised crime and terrorist offences. It also shows how principles of public interest immunity are used in those countries to protect sensitive intelligence material from being disclosed in criminal proceedings.[16]

1.2 Initial concerns

Not all commentators were in favour of lifting the ban. In particular, the then Interception of Communications Commissioner[17] Sir Swinton Thomas said in 2007 that:

> In my last Report I said that the question of the admission of intercept material in criminal proceedings had been discussed at some length in Parliament, the media and beyond. The aim of all concerned in the intercepting agencies is to use the material to best advantage to detect and prevent terrorism and serious crime. If it was a simple matter to change the law to allow intercept to be used evidentially without losing the very substantial benefits delivered by the existing intelligence only regime, I have no doubt that it would have been done many years ago. The truth is that there is no simple way of achieving this. I concluded by saying that I had no doubt that the balance of argument fell firmly against any change in the law, and that any change in the law, would, overall, be damaging to the work of the security, intelligence and law enforcement agencies.[18]

In his report reviewing the operation of the *Prevention of Terrorism Act* in 2006 (which was published on 19 February 2007[19]) Lord Carlile QC noted that much of the information on which decisions concerning control orders were based was derived from intelligence. He went on to say:

> The sources and content of such intelligence in most instances demand careful protection in the public interest, given the current situation in which a concerted and strategic response to terrorism (and especially suicide bombings) is needed. The techniques of gathering intelligence, and the range of opportunities available, are wide and certainly in need of secrecy. Human resources place themselves at risk – not

---

[15] Home Affairs Committee, *Terrorism Detention Powers*, 28 February 2006, HC 910-iii, available at: http://pubs1.tso.parliament.uk/pa/cm200506/cmselect/cmhaff/uc910-iii/uc91002.htm

[16] JUSTICE, *Intercept Evidence: Lifting the Ban*, October 2006, available at www.justice.org.uk

[17] As mentioned above, the Interception of Communications Commissioner reviews the issue and operation of warrants permitting the interception of mail and telecommunications and the acquisition of communications data by the intelligence and security agencies, Ministry of Defence and law enforcement organisations, and the arrangements for handling the material

[18] Sir Swinton Thomas, *Report of the Interception of Communications Commissioner for 2005-2006*, HC 315, 19 February 2007, available at: http://www.official-documents.gov.uk/document/hc0607/hc03/0315/0315.pdf

[19] Lord Carlile QC, *Second report of the independent reviewer pursuant to section 14(3) of the Prevention of Terrorism Act 2005* 19 February 2007, available at: http://www.official-documents.gov.uk/document/cm71/7194/7194.asp

> least, by any means, those who offer unsolicited information out of disapproval of conduct and events at which they may have been and might continue to be present.
>
> That is not to say that there might possibly be a few cases in which it would be appropriate and useful to deploy in a criminal prosecution material derived from public system telephone interceptions and converted into criminal evidence. Although the availability of such evidence would be rare and possibly of limited use, I restate that it should be possible for it to be used and that the Law should be amended to a limited extent to achieve that.[20]

During the *Serious Crime Bill's* proceedings in Committee in the House of Lords, the former Law Lord, Lord Lloyd of Berwick (who had carried out the review of anti-terrorist legislation which had preceded the introduction of the *Terrorism Act 2000*) sought to introduce an amendment that would have provided for the admissibility of intercept evidence in cases involving serious crime. In opposing Lord Lloyd's amendment, the then Home Office minister Baroness Scotland said the Government's position had always been that lifting the ban on intercept evidence would be an advantage only if it could be safely deployed. She went on to echo the view of the then Interception of Communications Commissioner, Sir Swinton Thomas, that lifting the ban in the way proposed by Lord Lloyd's amendments would cause grave damage to the UK's capability and that protection was vital.[21]

Baroness Scotland concluded by seeking to reassure peers that the issue had been rigorously examined and would continue to be rigorously examined during the continuing review. Lord Lloyd of Berwick subsequently withdrew his amendment but said he would bring the matter back at a later stage.[22]

When the Bill was considered on Report in the House of Lords on 25 April 2007, Lord Lloyd again moved amendments designed to enable the admission of intercept evidence in cases involving serious crime. His amendments were again opposed by the Government but they were agreed to on division by a majority of 61.

On 7 June 2007 the then Home Secretary, Dr John Reid, published the *Government Discussion Document Ahead of Proposed Counter Terror Bill 2007* in which he made the following comments about intercept evidence:

> The Government's position on intercept as evidence has consistently been that we would only change the law to permit intercept evidence if the necessary safeguards can be put in place to protect sensitive techniques and the potential benefits outweigh the risks.
>
> The right approach is to address this carefully and fully before deciding on whether to use intercept as evidence. That is what we are doing. However we believe that we now need to reach a conclusion on this issue. Therefore, subject to further discussions to agree the structure and timescale, I am today announcing that we will commission a review of intercept as evidence on Privy Counsellor terms.[23]

Lord Lloyd's amendments on intercept evidence were then removed in the Commons.

---

[20] *Ibid*, paras 34-35
[21] HL Deb, 7 March 2007, c302-303
[22] *Ibid*, c314
[23] Home Office, *Government Discussion Document Ahead of Proposed Counter Terror Bill 2007*, June 2007, p4

In January 2008, it was reported that Sir Paul Kennedy, the current Interception of Communications Commissioner, had concluded that "the benefits of any change in the law [to intercept evidence] are heavily outweighed by the disadvantages."[24]

The Intelligence and Security Committee spelled out the potential benefits and concerns in its Annual Report 2006–2007, published in January 2008. It focused on national security concerns, stating that:

> 111. The concerns of this Committee have centred on whether or not there is a net benefit, in terms of national security, from introducing intercept into the courts. At its simplest, it is a question of whether using intercept material in court would result in more terrorist convictions than are already achieved through its use to generate leads, and whether these would be sufficient to outweigh the possible reduction in the capability of the Agencies to identify the terrorists and disrupt attacks in the first place.
>
> 112. Those in favour of lifting the ban have argued that, logically, the prosecution must be able to take advantage of every piece of evidence it can when trying to secure the conviction of terrorists and serious criminals: if there is intercept that would help their case, then they should be able to use it. They argue that the Government should not be requesting Control Orders to contain terrorist suspects that it cannot successfully prosecute when it is not using all the available evidence. They also argue that the nature of intercept evidence can be instrumental in persuading a defendant to plead guilty or help the prosecution in other ways.
>
> 113. The Agencies, however, are adamant that their intercept capabilities must not be disclosed in court. If they were, criminals and terrorists would quickly learn what the Agencies can and cannot do, and would find means of avoiding detection, which would then damage their capability and coverage. Other countries, however, allow the use of intercept as evidence without any adverse impact on their security and intelligence capability, so what makes the UK different? GCHQ points to a unique combination of factors in the UK: The UK is the only country which has all three of the following things: an adversarial legal system, subordination to [the European Convention on Human Rights] and a strategic intercept and SIGINT capacity that is worth protecting.
>
> 114. In practice, because of the UK's adversarial legal system, the defence would be able to test the validity of evidence and thereby explore how it was obtained. As communications technology evolves (particularly internet protocol), we understand it may be difficult for the Agencies to be able to prove intercept to an evidential standard. In addition, whilst it may be possible to prevent defence probing of the actual technique, we understand that mere revelation of intercepted material could compromise sensitive capabilities: the Agencies, understandably, clearly wish to protect what they can and cannot do.
>
> 115. A further argument we have considered is the additional burden that would arise from a requirement to record and retain all intercept material of potential relevance to a future prosecution and, in the event of such a prosecution, to review that material for disclosure purposes. This would place a huge administrative and resource burden on the Agencies, which we consider they are ill placed to shoulder at a time when they are stretched trying to provide coverage of the terrorist threat to the UK.
>
> 116. **** [paragraph excised]
>
> 117. The Director of GCHQ summarised the test for allowing intercept:

[24] *The Guardian*, "Watchdog sides with MI5 to reject phone-tap evidence", 29 January 2008

… a change to allow intercept as evidence should be introduced only when doing so would have a net benefit in securing the safety and the security of the UK. By that I mean not just convicting and imprisoning criminals, but also preventing crimes and terrorist actions.

118. The issue, therefore, is whether permitting intercept as evidence would have a real long-term impact in terms of securing more convictions than already secured by the use of intercept for intelligence leads. Having not been shown the Home Office study on this, we have yet to see any hard evidence. Giving evidence to the Committee, GCHQ summarised its position on lifting the ban on the use of intercept material: *"So far we do not believe that anything proposed passes the test of doing more good than harm, and we are convinced that it would lead to a net reduction in our national ability to deal with crime and terrorism."*

119. The Home Secretary shared these concerns: *"There would be benefits in an ideal world. But I do not believe you could do this without a huge risk of a downside for our operational capacity in the long term, and I am very wary of winning the minutes but losing the hours.*

V. Intercept is of crucial importance to the capability of the Agencies to protect the UK, its citizens and its interests overseas. Any move to permit the use of intercept evidence in court proceedings must be on a basis that does not jeopardise that capability.

120. Whilst we have examined whether or not intercept should be admitted as evidence insofar as it relates to the work of the intelligence and security Agencies, we note that the Prime Minister has established a cross-party Privy Council review of the wider issue The review is being led by the Rt. Hon. Sir John Chilcott and includes the Rt. Hon. Alan Beith, MP, a member of this Committee. We have submitted our findings to this review.

1.3 The Report of the Chilcot Review

The Privy Counsellor Review, led by Sir John Chilcot, reported on 6 February 2008.[25] The BBC noted that "the committee produced its report after hearing from 40 individuals, including judges, security service officials, telecommunications experts and government ministers. It also received submissions from 12 countries where intercept evidence is admissible in court proceedings."[26]

The review concluded that intercept evidence should be used subject to a number of important conditions. The report set out 9 tests to be passed before any such evidence will be admitted in a court.

The report stated, *inter alia*, that:

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

---

[25] Privy Council Review of Intercept Evidence, January 2008, Cm 7324
[26] BBC Online, Checks and Balances for Intercept Use, 6 February 2008

4. These different views were in almost all cases strongly held, and in many instances have been the firm views of the organisations involved for many years. However, some of those involved have changed their views in the light of experience. The arguments they bring, for and against intercept as evidence, are by their nature asymmetric. Those in favour of intercept as evidence make their case on the basis of openly available material. Those who believe that the case has not been made, or that a model with the necessary safeguards has not been found, cannot put their case fully in public, as at least key parts of it rely on classified material, for example the nature, scale and benefit of the current use of intercept as an intelligence and investigative tool, and the risks to which it is exposed.[...]

It concluded that:

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

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

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

The Prime Minister made a statement on the same date, saying:

> Briefly, the report examines in detail both the potential benefits of accepting intercept as evidence and the risks that might arise from such acceptance. However it concludes that it should be possible to find a way to use some intercept material as evidence, provided – and only provided, that certain key conditions can be met. […] The report sets out nine conditions in detail. They relate to complex and important issues and include: giving the intercepting agencies the ability to retain control over whether their material is used in prosecutions; ensuring that disclosure of material cannot be required against the wishes of the agency originating the material; protecting the current close co-operation between intelligence and law enforcement agencies, which is crucial; and ensuring that agencies cannot be required to transcribe or make notes of material beyond a standard of detail that they deemed necessary. The committee that reported to us acknowledges that further extensive work is needed to see whether and how those and other conditions – intended to protect sensitive techniques, safeguard resources, and ensure that intercept can still be used effectively for intelligence – can be met. That is a unanimous recommendation that the Government accept, so we will proceed to develop a detailed implementation plan under which material might be made available for use in criminal cases in England and Wales. […] Designing a regime to meet the Chilcot conditions will require, as the committee notes, a substantial programme of work, covering legal, operational and technical issues. The work must involve and engage the intelligence agencies, Government Departments, the legal system, and those responsible for communications. […] The Chilcot team also told me they would not expect the work to be concluded in time to inform the Counter-Terrorism Bill currently before Parliament.[27]

In answer to a question by Andrew Dismore, the then Chairman of the Joint Committee on Human Rights, as to whether the Government would consider including enabling powers in the *Counter-Terrorism Bill*, the Prime Minister responded:

> That was not the recommendation of the Chilcot report. When I met the membership of the committee, we had a detailed discussion about some of those issues. If we said the enabling legislation could be introduced before we had reached a solution to some of the problems that had been raised, we would raise false expectations that we had such solutions. Those solutions still have to be found, and the legal and technical work must still be done.[28]

Moves to allow intercept evidence were immediately welcomed by the Law Society, JUSTICE, and, Liberty, all of whom argued that the Government's decision to allow the use of intercept evidence in court should help to reduce the length of time suspects need to be detained pre-charge.

In February 2009, Sir John Chilcot wrote to the Prime Minister, to provide a progress report.[29] Subsequently, then Home Secretary, Jacqui Smith, made a statement to the House on this issue:

> The Privy Council of intercept as evidence was published on 30 January 2008.

---

[27] HC Deb, 6 February 2008, c959-961
[28] *Ibid*, c968
[29] http://www.parliament.uk/deposits/depositedpapers/2009/DEP2009-0429.pdf

> In his statement to the House of 6 February 2008 my Right Honourable Friend the Prime Minister affirmed his commitment to the principle of using intercept as evidence and the case for doing so provided that national security could also be protected. He also agreed that the programme of work recommended by the Report be taken forward, with the objective of legislation. At the same time, the Privy Council Review itself, acknowledged that before legislation could be brought forward, further extensive work was required.
>
> I am pleased to be able to report on progress. I am also having placed in the House Libraries copies of a progress report to my Right Honourable Friend the Prime Minister on behalf of the Advisory Group of Privy counsellors, comprising the Right Honourable Sir John Chilcot, the Right Honourable Sir Alan Beith MP, the Right Honourable Michael Howard QC MP, and my noble Friend the Right Honourable Lord Archer of Sandwell. I should like to express my thanks to the Advisory Group for their diligent and constructive support for this programme of work. I should also like to echo their praise for the "commitment and thoroughness with which the interception community has sought to address the issues".
>
> The Privy Council Review rightly recognised that interception is of vital importance to public protection and national security. It also recognised that the issues raised by the potential use of intercept product in evidence are complex. This has proved to be the case, as the Advisory Group's report makes clear. However, we have now reached the end of the programme's first phase, with work to design in detail the model recommended by the Privy Council Review, now largely complete. Work is now in hand to flesh out the detailed guidance required in advance of testing the practicalities of the model.
>
> However, it is clear a number of key issues remain to be resolved if the objective of facilitating the prosecution of terrorist and other serious crime with the assistance of intercept as evidence is to be achieved. As the Advisory Group observes there is an intrinsic tension between meeting legal needs and the operational requirements identified by the Privy Council Review. It is also not yet clear whether the key safeguard of our being able to revert to the current regime should implementation fail would itself be legally sustainable.
>
> The Government agrees with the Advisory Group that "securing the intended increase in successful prosecutions while ensuring fairness of trials remains difficult and may not prove possible in most complex cases". The Government agrees on the importance of a further stage of work being taken forward urgently to test the viability of the model developed.
>
> The Government's intention remains to be in a position to bring forward legislation for use of intercept as evidence as soon as possible. However, it believes, given the importance of interception for national security, including the ability to prevent and disrupt serious crime and terrorism, that if the results indicate that there is no practical solution, they should be accepted. Equally, if it is necessary to take further time to iron out the detail of an apparently workable solution, we should do so rather than be driven by the legislative timetable.[30]

A further statement was issued by Alan Johnson, in July 2009. He said:

> In her written ministerial statement to the House on 12 February, Official Report, columns 87-88WS, the then Home Secretary, Member for Redittch, the right hon.

[30] HC Deb 12 February 2009, c87-8WS

> Jacqui Smith, provided a progress report on the work being undertaken following the publication of the Privy Council review of intercept as evidence in January 2008.
>
> I am pleased to be able to provide a further update, and to explain why I have concluded it is right to provide the House with a full report after the summer recess.
>
> Since February, detailed work has focused on testing the practical impact and effect of the model developed. This work has been undertaken in concert with experienced independent legal practitioners. The programme is now complete, and work is now in hand to draw the emerging conclusions and test their validity. The Advisory Group of Privy Counsellors, the right hon. Sir John Chilcot, my noble Friend the right hon. Lord Archer of Sandwell, the right hon. Member for Berwick-upon-Tweed (Sir Alan Beith) and the right hon. and learned Member for Folkestone and Hythe (Michael Howard) is following this closely. Indeed they also see merit in seeking further advice on key points for, as they noted in their interim report in February, the issues are complex. I know they share my determination to get this right. I should like to thank them for their continuing commitment and invaluable contribution.
>
> I look forward to discussing with them the final conclusions of the programme. I shall then provide a formal report to Parliament on the full findings of the work programme, and the Government's decision in the light of them, soon after the return following the summer recess.[31]

2 Difficulties with implementation

2.1 Some new issues

In May 2009, the Labour Government, in its *Reply to the Fourth Report of the Independent Reviewer Pursuant to Section 14(3) of the Prevention of Terrorism Act 2005*[32], indicated that whilst an implementation team was "taking work forward with urgency", "key legal and operational issues remain to be resolved". In particular, it highlighted the fact that a review of nine current or former control order cases had been conducted by independent senior criminal counsel and that he had concluded that:

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

---

[31] HC Deb 16 July 2009, c59WS

[32] UK Government, Reply *to the Fourth Report of the Independent Reviewer Pursuant to Section 14(3) of the Prevention of Terrorism Act 2005*, May 2009, Cm 7624, p6

In November 2009, Lord Carlile produced a report into the conduct of Operation Pathway, an anti-terror swoop on 11 men in north-west England. Lord Carlile made some observations on intercept evidence during the course of that report, noting that:

> Despite my willingness for it to be introduced in appropriate circumstances, I have yet to see material to justify the conclusion that the permitting of such evidence in terrorism cases would do more good than harm. [...] I believe that this debate should now be drawn to a conclusion, against the introductions of intercept evidence in terrorism cases, with an undertaking to keep the matter under review in the light of any changing circumstances.[33]

On 10 December 2009, it was reported that the Home Office had concluded that the reports they had received were such that "no responsible government" could proceed with implementing the introduction of intercept evidence on the basis of the proposed model. Alan Johnson said that "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."[34]

He added: "because of the additional demand on resources to make intercept as evidence admissible in court, this model could jeopardise national security and damage our ability to bring terrorists and other serious criminals to justice."[35]

The former judge, Sir Geoffrey Grigson, who had participated in mock trials to test the admissibility of the evidence was quoted as having said that allowing the material could also have serious operational implications:

> With intercept, that will almost certainly require disclosure to the defence of information regarding techniques used by agencies and their capacities. Disclosure of such material would cause serious damage to the intelligence processes.[36]

However, the BBC said that a "senior Whitehall source" had indicated that this was not the "death knell" for the use of intercept evidence.[37]

In a statement to Parliament, the then Home Secretary stated that:

> **Intercept as Evidence**
>
> **The Secretary of State for the Home Department (Alan Johnson):** The Government have 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 those individuals who seek to do us harm.
>
> 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 security. He set in train the necessary implementation process and

---

[33] *The Times* "Anti-terror watchdog warns against intercept evidence", 24 November 2009 and *The Guardian*, "Ban intercept evidence in terror trials, advises Lord Carlile", 24 November 2009
[34] *The Times* "Intercept evidence plans beset by flaws", 10 December 2009
[35] *BBC Online*, "Using intercept evidence in court 'not yet viable'", 10 December 2009
[36] *BBC Online*, "Using intercept evidence in court 'not yet viable'", 10 December 2009
[37] *Ibid*

established an advisory group, comprising the right hon. Sir John Chilcot, the right hon. Member for Berwick-upon-Tweed (Sir Alan Beith), the right hon. and learned Member for Folkestone and Hythe (Mr. Howard), and my right hon. And noble Friend Lord Archer of Sandwell, in order to help safeguard intelligence capability and protect the public.

In my written ministerial statement to the House of 16 July I provided an update on the progress of the implementation programme. I said that I would make a formal report to Parliament on the results and conclusions after end of the summer recess.

I am today publishing a Command Paper setting out the work programme's findings and conclusions. Copies will be available in the Vote Office. I am also placing in the Libraries of both Houses copies of a separate report to my right hon. Friend the Prime Minister by the advisory group. The Prime Minister and I are grateful to the advisory group for its work. I echo their recognition both of the complexity and sensitivity of the work programme and the commitment and thoroughness of officials in undertaking it.

Any implementation of intercept as evidence must, as set out in the original Privy Council review, ensure that trials continue to be fair and that the operational requirements to protect current capabilities are met. As noted in the advisory group's interim report to the Prime Minister, reported in my predecessor's written ministerial statement of 12 February and placed in the Libraries of both Houses, there is an intrinsic tension between these legal and operational requirements.

The work programme set out to develop a model for intercept as evidence that successfully reconciled these requirements, based on the approach recommended by the Privy Council review. This model has been subject to extensive practical testing, with the close involvement of senior independent legal practitioners. This testing has demonstrated that the model, if fully funded, would be broadly consistent with the operational requirements. However, it would not be legally viable, in that it would not ensure continued fairness at court. This has been confirmed by a recent European Court of Human Rights case (Natunen v Finland). The result would be to damage rather than enhance our ability to bring terrorists and other serious criminals to justice.

These findings are disappointing. In the light of them, the Government conclude, as does the advisory group, that the model does not represent a viable basis for implementation. However, the Government also share the advisory group's view that the potential gains from a workable intercept as evidence regime justifies further work. We therefore welcome the group's suggestion of three areas of analysis, beyond the scope of the original work programme, intended to establish whether the problems identified are capable of being resolved. These areas are to examine:

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.

The Government agree with the advisory group that while continuing to seek innovative and imaginative approaches, these should not be at the cost of the operational requirements, and hence national security or public protection. I am grateful for the advisory group's agreement to continue in its current invaluable role and for agreeing to be similarly engaged on interception related matters that have arisen in the context of the Coroners and Justice Bill.

> The Government will report the results of this activity to Parliament before the Easter recess.[38]

The abovementioned Command Paper *Intercept as Evidence* is available online.[39] Amongst other things, it indicated that the work programme and model that had been tested was based on an approach known as "Public Interest Immunity Plus" which the Privy Council review had concluded was the most likely to be legally viable.[40]

2.2 The case of *Natunen v Finland*

One issue raised in the *Intercept as Evidence* paper was the impact of the case of *Natunen v Finland* (application no. 21022/04). In that case, the European Court of Human Rights determined (unanimously) that that there had been a violation of Article 6 (right to a fair hearing) of the *European Convention on Human Rights*, on account of recorded telephone conversations obtained through secret surveillance not having been disclosed at the applicant's trial for drug trafficking. The summary of the case provided in the press notice issued by the court on 31 March 2009 said that:

> Mr Natunen and two other persons were suspected of trafficking in drugs. In October 2001 the police seized amphetamines from the possession of one of the two other suspects. According to the prosecution, they had arranged for the drugs to be hidden in a truck and transported from Estonia to Finland. They were all subsequently charged with aggravated drug offences.
>
> All of the accused denied the charges; they stated that they had intended to buy weapons, not drugs. They submitted that this could be verified through their telephone conversations in the relevant period. The police, having collected evidence through telephone surveillance, informed Mr Natunen that all the calls related to the drugs offence – 21 recorded telephone conversations and 7 recorded text messages – had been included in the pre-trial investigation case file. Mr Natunen argued, however, that many other conversations, which had been relevant and could have proven his innocence in respect of the drugs offence, had been excluded from the file and had never been disclosed to him.
>
> In 2002, the domestic courts, relying on the telephone recordings included in the file, found Mr Natunen guilty as charged and sentenced him to seven years in prison. On appeal he argued that the conversations which had not been included contained information proving his innocence; the prosecution maintained, however, that – in accordance with domestic law – those recordings had been destroyed as they had not been connected to any other offence which would have allowed the police to retain them without breaching the law. [...]
>
> **Decision of the Court**
>
> The Court first observed that the destruction of some of the recordings obtained through telephone surveillance had made it impossible for Mr Natunen to have his claim of innocence verified. The Court also noted that the recordings had been destroyed by the police at the pre-trial stage without having consulted Mr Natunen or his lawyer and without having given the courts the possibility to assess their relevance.The Court found that that destruction had been a direct result of the application of the relevant domestic legislation in force at the time, which had been defective as it had allowed information supporting the innocence of the suspect to be

[38] HC Deb, 10 December 2009, c31-32WS
[39] Home Office, Intercept as Evidence: A Report, Cm 7760, December 2009
[40] *Ibid*, para 6 and see also Annex B

> destroyed before the case had been decided. While the Court noted that the legislation had since been amended, and the defect eliminated, it held that there had been a violation of Article 6 § 1 taken together with Article 6 § 3 (b) as this legislative amendment had come too late for Mr Natunen.[41]

The paper concluded that (partly as a result of this judgment) the unanimous legal advice was that the model that had been developed in the work programme would not be legally viable. It indicated that:

> 11. In order to comply with the fourth and fifth operation 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 decision 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.[42]

On 10 December 2009, following the then Home Secretary's abovementioned Written Ministerial Statement, JUSTICE issued a press release criticising the continuing delays in lifting the ban on the use of intercept evidence in legal proceedings:

> The UK is the only country in the common law world to ban the use of intercept material in legal proceedings. Intercept evidence is used regularly in Australia, Canada, New Zealand, the United States and South Africa in criminal prosecutions, including cases of terrorism and serious organised crime.
>
> The failure to allow intercept evidence in open court has led the government to resort to a variety of exceptional measures, including the introduction of indefinite detention without charge in 2001, the introduction of control orders in 2005, and the power to order a secret inquiry in place of an inquest in 2009.

Dr Eric Metcalfe, JUSTICE's Director of Human Rights Policy said:

> Nearly two years since the Chilcot report, the government still hasn't figured out how to lift the ban on intercept evidence. Intercept evidence may not be a magic bullet, but it isn't rocket science either. It is well past time that this evidence was made admissible in UK courts.[43]

3 Recent Developments

On 18 March 2010, the Intelligence and Security Committee's Annual Report for 2009-2010 was laid before Parliament by the Prime Minister. The Report made the following comments regarding intercept evidence:

> 58. Since our last Annual Report, work (led by the Home Office) to examine whether a system could be devised to enable the use of intercepted material in court, which simultaneously satisfied the requirements for a fair trial and safeguard national security, has continued. On 10 December 2009 the Home Secretary published a

[41] European Court of Human Rights, Press Notice, 31 March 2009
[42] Home Office, Intercept as Evidence: A Report, Cm 7760, December 2009
[43] Justice press release, *JUSTICE criticises government delays over intercept evidence*, 10 December 2009

> further update report. The report concluded that the model which had been developed and tested would not be legally viable and that:
>
> *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.*
>
> 59. The report went on to note that the implementation of the original legal model would in fact "*weaken and not enhance our ability to protect the public and to identify and bring the guilty to justice*".
>
> 60. However, further work would be done on three areas that were outside the scope of the original programme which might address some of the current failings. These areas are: further enhancing judicial oversight, exploring options for the full retention of interception material, and considering whether advances in technology could make full retention and review more manageable. The results of this additional work are expected to be reported to Parliament before the Easter recess in 2010.
>
> **H. There has now been a comprehensive examination of the issues involved in allowing intercept material to be adduced as evidence in the UK. That it has failed to provide a viable model is unsurprising, given the complexities of the issues involved. We await the outcome of the further work now being done. We recommend that if this too fails to provide a workable solution then the issue should be considered closed.**[44]

In its response to the Report, the then Government said:

> The Government welcomes the Committee's recognition of the comprehensiveness of the work currently being led by the Home Office. The findings of this work are intended to be announced shortly and will undoubtedly determine the shape of future work on intercept as evidence. It remains the Government's desire to find a way to implement intercept as evidence, providing it does not jeopardise the protection of the public or national security.[45]

Alan Johnson's Written Ministerial Statement of 10 December 2009 indicated that the advisory group established to look at the use of intercept evidence in legal proceedings would be undertaking further work in this area. He said that he would report the results of this activity to Parliament before the Easter 2010 recess. On 25 March 2010, Mr Johnson made the following statement:

> **The Secretary of State for the Home Department (Alan Johnson):** My written ministerial statement of 10 December 2009, *Official Report*, column 31WS reported the conclusions of the work programme set in train following the Privy Council review of January 2008, to implement the use of intercept as evidence, consistent with protecting the public and national security. This concluded that the "PII Plus" model of IAE, recommended for further work by the Privy Council review, would not be legally viable, and would worsen rather than enhance our ability to bring the guilty to justice. The Advisory Group of Privy Counsellors (the right hon. Sir John Chilcot, the right hon. Member for Berwick-upon-Tweed (Sir Alan Beith), the right hon. and learned Member for Folkestone and Hythe (Mr. Howard), and my noble Friend the right hon. Lord

---

[44] Intelligence and Security Committee, *Annual Report 2009-2010*, March 2010, Cm 7844

[45] Cabinet Office, *Government Response to the Intelligence and Security Committee's Annual Report 2009–2010*, March 2010

Archer of Sandwell) established to advise on the work programme, agreed with this conclusion.

My written ministerial statement confirmed the Government's commitment to report back on further scoping analysis, intended to establish whether the problems identified were capable of being resolved, prior to the Easter recess. The areas to be examined were:

> 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.

I am having placed in the House Libraries copies of a progress report to my right hon. Friend the Prime Minister on behalf of the Advisory Group.

The findings underline the complexity and difficulty of the issues raised. None of the approaches examined successfully reconcile the requirements for trials to remain fair with those necessary to protect operational capabilities. In some cases the problems are such that further work is not justified. In some others the position may be less categorical. Reflecting this, the Advisory Group has suggested further, more focused work building on that undertaken previously and intended to establish whether the remaining approaches could be implemented in way that is operationally sustainable and affordable. The Government agree that this would be useful.

I should like to express my thanks to the Advisory Group for their continued contribution to this programme of work.[46]

The progress report referred to in the above statement made the following comments:

> The Advisory Group remains of the view that the use of intercept as evidence in criminal proceedings would be a valuable prize but at the same time it believes that this must not be at the expense of the operational requirements necessary to protect a capability vital to the nation.
>
> None of the approaches examined in this further phase of scoping work successfully reconcile the requirements for trials to remain fair with those necessary to protect the public and national security. In some cases the problems are such that further work is not justified. It is clear that the legal and operational challenges around the **'keys to the warehouse'** approach are insurmountable, and that **'enhanced judicial oversight'** is very unlikely to overcome the problems of unfairness at trial identified for the 'PII Plus' model. Similarly, **technology enabled review** does not at present offer a way forward – although it may in time potentially mitigate some of the operational burden involved in undertaking review.
>
> This suggests that further work might most productively be focussed on two areas which assume full retention. **'Review pursuant to defence-requests'** would be problematic, but it may be worth exploring the extent of the issues raised and scope to address them consistent with the operational requirements. Similarly, **'indexing, gisting and summarising'** has the advantage of being broadly consistent with [Criminal Procedures and Investigation Act 1996] processes and although not consistent with all of the operational requirements it would be worth examining the scale of possible impacts and scope to mitigate these.

---

[46] HC Deb 25 March 2010 cc61-62WS

It is, or course, likely to be for new or returning Ministers to consider next steps in the light of the ongoing security situation and economic climate. However, we believe that further work building on that done to date would be of value, the most promising avenues to explore being:

- Examining in more depth the operational, legal and public policy issues surrounding a full retention store.
- A more detailed assessment of the operational and financial impacts of alternative review based on either 'indexing, gisting and summarising' and 'review pursuant to defence-requests'.
- A validation of the findings on the prospects for technology enabled review to make full retention and review more manageable.[47]

The Parliamentary Joint Committee on Human Rights also issued a report on 25 March 2010. It said, amongst other things, that:

> 100. On 4 February 2010 we received an informal briefing from the "Intercept as evidence implementation team". We are grateful to them for keeping us informed and for their informative presentation. We do not underestimate the practical difficulties which are presented by relaxing the prohibition on the use of intercept as evidence. We also recognise the considerable amount of work which has gone into trying to develop a viable legal model for doing so. However, **it has become increasingly clear to us that the roadblock to progress is certain of the operational requirements which were stipulated by the Chilcot Review. In particular, the insistence on ongoing agency discretion over the retention, examination and transcription of intercept material (the fourth and fifth operational requirements) makes a legally viable regime impossible given the clear requirements of Article 6 ECHR.**
>
> 101. **We welcome the fact that the advisory group is continuing to explore ways of allowing intercept to be admitted as evidence, but unless these two operational requirements are revisited the next stage of the review is, in our view, already doomed to failure. We do not think the Government can be surprised by the decision of the European Court of Human Rights in *Natunen v Finland*: it has long been clear that Article 6 ECHR requires a full retention regime or judicial control over what may be discarded. We understand the agencies' anxieties about ceding their discretion in favour of judicial control, but, as we have seen in other contexts, this is an inevitable consequence of the agencies engaging with legal processes. In our view, the rule of law requires no less.**
>
> 102. **We do not see any difficulty in principle with independent judicial control over what material may be discarded. We therefore recommend that the fourth and fifth operational requirements of the Advisory Group of Privy Counsellors (requiring ongoing agency discretion over the retention, examination and transcription of intercept material) be revisited in the next stage of its work. Otherwise, we are concerned that the intelligence and security services continue to exercise a de facto veto over this beneficial reform by stipulating pre-conditions which are impossible to meet.**[48]

---

[47] Letter from the Advisory Group of Privy Counsellors to the Prime Minister regarding intercept as evidence, March 2010, DEP2010-0845

[48] Joint Committee on Human Rights, Counter-Terrorism Policy and Human Rights, (Seventeenth Report) Bringing Rights Back In, HC 111, 25 March 2010

3.1 The Coalition Government's Approach

In May 2010, the new Government published its coalition agreement, which stated "We will seek to find a practical way to allow the use of intercept evidence in court".[49] This commitment has been welcomed by civil liberties campaigners. For example, JUSTICE said:

> 53. We remain of the view that the case for lifting the ban on intercept is as strong as ever, not least because of the prominent role played by intercept material (ultimately obtained from California) in the conviction of three men of conspiracy to blow up transatlantic airliners in September 2009, as well as the most recent decision of the Special Immigration Appeals Commission in the case of Abid Naseer earlier this month. The use of intercept as evidence would be a major step towards closing the gap between suspicion and proof that has been the engine of so many disproportionate measures adopted since 9/11, including indefinite detention, precharge detention and control orders.
>
> 54. Since 2008, we have met the Home Office team working on the implementation of the Chilcot report on two occasions, and have made clear our view that it is perfectly feasible to introduce legislation allowing the use of intercept material in criminal and civil proceedings in a manner that would both protect sensitive details about interception capabilities while remaining compatible with the European Convention on Human Rights.[50]

Liberty also welcomed the commitment:

> The admissibility of intercept evidence in criminal proceedings is long overdue. While recognising the difficulties and sensitivities involved, we believe that it is entirely possible for a practical approach to the use of intercept to be found – drawing on the experience of other common law jurisdictions that do the same the world over.[51]

The issue was raised following a statement on the review of counter-terrorism and security powers. In the course of that debate, the Home Secretary, Theresa May, indicated that intercept as evidence was not being considered as part of the Government's review of the counter-terrorism legislation, but remained within the purview of the Privy Council group. She said:

> The previous Government set up a process to consider intercept evidence, and a Privy Council group is in existence to do that. [...] I want to talk to it about how we can take that issue forward in the best and most appropriate way, and I think it is better to do that over time rather than shoehorn it into this review.[52]

A Written Ministerial Statement, setting out the Coalition Government position, was made on 26 January 2011. It stated that:

> **Secretary of State for the Home Department (Theresa May):** The lawful interception of communications is a vital tool for tackling the threat posed by terrorism and other serious crime.
>
> The Coalition Government is committed to building on this by seeking to find a practical way to allow the use of intercept evidence in court.

---

[49] Cabinet Office, *The Coalition: our programme for government*, May 2010, p24
[50] Justice, *Response to the Coalition Programme for Government*, May 2010
[51] Liberty, *Liberty's analysis of the Coalition Programme for Government*, 20 May 2010, p6
[52] HC Deb 13 July 2010 c808

> The issues are complex. Because of this a first step has been to review previous analysis, including that in the Privy Council review (Cm 7324) and in 'Intercept as Evidence a report' (Cm 7760). Having done so, the Government is now in a position to set out next steps.
>
> As recognised in the Privy Council review the State has an overriding duty to protect the public, including from threats such as international terrorism and serious organised crime. Bringing prosecutions against and securing convictions of offenders is an important means of doing so.
>
> Equally, the effective use of intercept as intelligence already makes a vital contribution to public protection and to national security more widely.
>
> Therefore, the programme of work to be undertaken will focus on assessing the likely balance of advantage, cost and risk of a legally viable model for use of intercept as evidence compared to the present approach. The intention is to provide a report back to Parliament during the summer.
>
> Recent work on intercept as evidence has benefited significantly from the experience of the Advisory Group of Privy Counsellors, comprising the Right Honourable Sir John Chilcot, the Right Honourable and noble Lord Archer of Sandwell, my noble friend, the Right Honourable Lord Howard of Lympne and the Right Honourable Sir Alan Beith MP. I am pleased to be able to confirm that the members of the Advisory Group have, at my request and that of the Prime Minister and Deputy Prime Minister, agreed to continue to provide assistance and oversight.

The Justice and Security Green Paper

A Green Paper entitled Justice and Security (Cm 8194) was published on 19 October 2011. The paper contains a number of proposals which the Government argues "would better equip our courts to pass judgment in cases involving sensitive information" and "protect UK national security by preventing damaging disclosure of genuinely national security sensitive material."

The paper did not contain any new proposals on the potential use of intercept evidence, although the paper did note that "the Government is committed to seeking a practical way of allowing the use of intercept as evidence in court." The Government argued that:

> **Intercept as evidence: a separate challenge and a separate Government project**
>
> Intercept as evidence (IAE) is the proposed use of intercept material (for example telephone calls, emails and other internet communications) obtained under a RIPA warrant as evidence in criminal proceedings.
>
> Both the Green Paper and work on IAE reflect the Government's commitment to justice, openness and transparency, and its desire that, wherever possible, evidence is brought before the courts. However, as made clear when it was announced, the Green Paper is not the appropriate means for addressing the Government's commitment to seeking a practical way of adducing intercept evidence in court. Although some of the issues may appear related, in practice the topics are clearly distinct. Seeking to group them would complicate and delay progress rather than expedite it. Importantly:
>
> - First, the Green Paper is centred on civil proceedings, addressing specific issues raised by recent court judgments. In contrast, work on IAE is centred on the practicalities of introducing its use across serious criminal proceedings. Intercept material can already be adduced in certain civil proceedings, such as SIAC and Proscribed Organisations Appeal Commission cases.

- Second, the Green Paper is centred on the issue of protecting sensitive material. While this must also form an essential feature of any viable IAE regime, the requirements of Article 6 of the ECHR are different – and more demanding – in the criminal than the civil sphere. So bespoke solutions need in any event to be developed for both circumstances.

- Finally, the issues to be addressed in developing a legally compliant and operationally practical approach to IAE go much wider than protecting sensitive material alone – essential though this is.

Reflecting this, work on IAE continues to be overseen by the cross-party Advisory Group of Privy Counsellors.[53]

4 International Comparators

One issue that has frequently been raised is the fact that many other countries have some mechanism for the use of intercept evidence in their courts. Substantial information about both common law and European jurisdictions is available in many of the documents linked in this paper. Notably, in its 2006 Report, *Lifting the Ban*[54], the NGO JUSTICE argued:

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

It also contended that:

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

Subsequently, the Privy Council Review[55] considered some of these international comparators in the course of its initial report in 2008[56]. It said:

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

---

[53] Cabinet Office, Justice and Security (Cm 8194), p 11
[54] See in particular, pp 45-68
[55] Privy Council Review of Intercept Evidence, January 2008, Cm 7324
[56] See in particular, pp 31-42

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

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

- The examining magistrate system of criminal proceedings combines investigative and judicial functions within one role, with the examining magistrate able to authorise intercepts to develop the investigation for which he/she is responsible. Once the case comes to trial, defence questioning of this case is far less rigorous than under the UK system. This means that the risks of disclosure of sensitive techniques or content is considerably lower than it would be in the UK, whilst at the same time being less open to ECHR Article 6 challenge, as the intercept has been produced as part of a judicially overseen enquiry.

- In France, The Netherlands and Spain, law enforcement agencies' efforts to combat serious organised crime and terrorism receive less support from their security and intelligence agencies than is the case in the UK. We have concluded that the price of adopting such a clearly split system of intercept in the UK would be a significant reduction in the amount of day to day support provided to serious crime investigations in the UK by the intelligence services' intercept capabilities.

- *** [material excised]

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

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

- The interwoven nature of the current use of intercept by UK law enforcement and intelligence agencies, to combat serious crime and terrorism, and the cooperation and support they provide to each other does not exist to the same degree in Australia, Canada or the United States.

- These countries are not bound by ECHR. Such aspects of their systems (such as transcribing only that material which the law enforcement agencies intend to use in court, and using closed hearings in criminal proceedings) would need to be judged ECHR Article 6 compliant if they were to be replicated in any UK system.

- US prosecutors are able to use intercept material together with plea bargaining, to "turn" defendants and to secure early guilty pleas. This experience might not be replicated in the UK, where plea-bargaining in the US sense is not permitted.

In particular, the report focused on the experience of the Republic of Ireland:

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

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

(as An Garda Síochána is also the security service). Intercept applications are authorised by the Minister for Justice, Equality and Law Reform.

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

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

137. ***

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

The most recent Home Office Report, *Intercept as Evidence*[57] revisited the argument. It claimed that:

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 cooperation 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.

[57] Home Office, Intercept as Evidence: A Report, Cm 7760, December 2009