Evidence for Change
Lifting the ban on intercept evidence in court

Britain is almost alone in not allowing intercept evidence to be used in terrorism and other criminal trials. Without it, serious criminals may go free and terrorism suspects may be detained without charge. The weight of informed opinion is that the ban on the use of intercept evidence should be lifted. The security services disagree. Isn’t it time to let Parliament decide?

Introduction

The interception of communications is at the centre of government’s strategy to identify and frustrate terrorist conspiracies and other serious criminal activities. The Rules of the Game, our report on counter terrorism laws and practice, recognises that surveillance and the interception of communications must necessarily be in the front line of attempts to prevent further terrorist outrages. We cannot prevail without it.

But though the gathering of intercept information by the intelligence and law enforcement agencies from telephone calls, emails, fax and post is vital in identifying terrorists and other serious criminals, the government refuses to allow it to be used to bring them to trial. This is the result of section 17 of the Regulation of Investigatory Powers Act 2000. Its purpose is to protect the state’s interception activities from disclosure. Its effect is that if there is no other evidence against suspects they must either be released without charge, or in the case of suspected terrorists, detained without charge under control orders or by improper use of the immigration laws.

The UK is the only country in the common law world that almost wholly prohibits the use of information obtained by the security forces and police by intercepting communications as evidence in criminal proceedings. The United States, Australia and Canada, for example, allow and use intercept evidence in criminal proceedings, as has the International Criminal Tribunal at The Hague hearing cases against Yugoslav war criminals in 2004. In the United States, intercept evidence has been used to convict those involved in terrorism and serious crime, including Al Qaeda plotters and five mafia godfathers in New York.

Even in the British courts intercept evidence may be admitted in certain limited circumstances, including if it derives from foreign sources. In October 2006, for
example, intercept evidence from Austria, Belgium and Italy played a vital role in securing the convictions of a ring of Turkish people traffickers. But it was only admissible in court because it was obtained lawfully by the foreign law enforcement agencies.

We are reliably assured that the government would like to make intercept evidence available in court. The Prime Minister stated in the House of Commons, just two weeks after the 7 July attacks, that it is on the advice of the security services that the government still upholds the ban on its use in court:

It is not an issue on which there is an objection in principle to using such evidence. On the contrary, as a matter of principle, I would prefer to use it rather than not use it, but we have to take account of our advice.3

Last September, after being impressed on a visit to the United States by the gaoling of the five mafia godfathers through the use of intercept evidence, the Attorney General told the BBC that it was a ‘vital tool’ for use against serious criminals, including terrorists:

We do have a need to use intercept in court if we are going to give ourselves the chance of convicting some of the most dangerous and prolific criminals in this country.

He acknowledged the ‘legitimate concerns’ of the security forces, but said that they should be dealt with.4

This paper surveys the case for and against the use of intercept evidence in criminal proceedings. We conclude that the current absolute ban is unnecessary and counter productive; we are persuaded that the legitimate concerns of the intelligence services must be met; and we recommend that the blanket ban should be lifted.

**Intelligence concerns**

If reform is to be achieved, it is most important that the concerns of the intelligence services should be taken seriously. Their objections fall into three main categories, but the central fear is that use of intercept evidence in court would endanger their sophisticated capabilities, agents and informants and could entail great losses in the longer run. However, the experience both of the use of public interest immunity (PII) certificates in the British courts to protect sensitive information and similar procedures in seven other common law countries, surveyed by JUSTICE, suggests that means can be found to prevent their methods and sources from being compromised by the considered use of intercept evidence in court.

JUSTICE found that public interest immunity principles, which are well established in the UK courts, work well in these countries to ‘prevent the unnecessary disclosure of sensitive intelligence material’, intercept techniques, capabilities and sources.5

On the other hand, the refusal to allow this evidence to be used in court means that some serious criminals go free, and that some terrorist suspects are or will be detained without charge. A ‘shadow’ system of criminal justice, by which terrorist suspects are detained without trial by special courts, has been created which subverts the basic principles of British justice and violates human rights. This process arguably contributes to the essential argument of the extremist elements within the British Muslim communities that the United Kingdom persecutes Muslim people at home and abroad. The government must do all it can in the interest of all citizens to restore this country’s system of adversarial criminal justice to protect fair trial and due process, to convict the guilty and acquit the innocent.

The ban is made all the more objectionable as the government has consistently justified three phases of its counter terrorism measures that set aside due process and human rights by reference to the difficulties of producing evidence in terrorism cases: the indefinite detention of foreign suspects without trial (and later their improper detention under the 1971 Immigration Act);

the imposition of control orders on suspects; and the raising of the maximum period of pre-charge detention from 14 to 28 days.6 We cannot state categorically that intercept evidence would have been available for prosecutions against the detainees, but it seems likely that it could have been. If it had not, then it is reasonable to ask what information precisely there was against these suspects; and the case for using extraordinary legal measures appears weakened further.

The groundswell of informed opinion over the past decade reinforces the Prime Minister’s preference in principle for reform and the Attorney General’s wish to find ways of satisfying the security forces’ concerns about disclosing information that could assist criminals. Lord Lloyd of Berwick, the former law lord who conducted the government’s review of counter terrorism legislation for a report in 1996, is introducing a Private Member’s Bill in the House of Lords, that receives its second reading on Friday 16 March, to lift the ban. (He has also tabled an amendment to similar effect to the government’s Serious Crime Bill, which is currently before Parliament.) It is to be hoped that the government will take over this Bill and see it into law after full parliamentary scrutiny and debate; or otherwise, that the House of Lords will pursue the Bill vigorously.

**Intercept evidence**

The Regulation of Investigatory Powers Act 2000 (RIPA) authorises the covert interception of telephone calls, either landline or from mobiles, email, fax and post, by the intelligence services, police and law enforcement agencies and other bodies. The purpose is solely to gain information on the activities of those who are suspected of being involved in serious crime, terrorist plots or other threats to national security. But section 17 of the Act prohibits the use of any intercept evidence obtained that discloses the fact of the interception or the substance of
any communication (superseding the similar provision in section 9 of the Interception of Communications Act 1985). This ban does not apply to other information gained from covert surveillance, such as the ‘bugging’ of suspects using a concealed microphone, or footage from hidden cameras.

There are legitimate concerns about the invasion of privacy by such activities, but it is justified on the grounds it provides vital information in the fight against serious crime and terrorism – and, indeed, in defence of ‘the right to life’, the government’s prime human rights obligation. RIPA introduced safeguards to ensure that the interceptions are lawful and proportionate. Section 5 of the Act stipulates that the Secretary of State (usually the Home Secretary) may issue interception warrants only if she or he believes it to be necessary (reflecting Article 8 of the ECHR ‘necessary in a democratic society’) in the interests of national security, the prevention or detection of serious crime or to safeguard the economic well-being of the UK. Warrants may also be issued in accordance with an international mutual assistance agreement.

The security forces and police may intercept communications without a warrant – for example, when a kidnapper is telephoning relatives of a hostage, or communications with a prisoner or high-security psychiatric patient. These intercepts are admissible in court under section 18 of RIPA: Ian Huntley was convicted of the Soham murders in December 2003 partly on the basis of intercepted telephone calls between him, his girlfriend and mother.

Senior officials may sign warrants on behalf of the relevant Secretary of State in urgent circumstances and similarly the Secretary of State or officials may modify existing warrants. Applications are normally granted, although there are rare cases of refusal which are officially seen as evidence that the Secretary of State does not apply a ‘rubber stamp’.7 David Blunkett’s memoirs give a brief insight into the process, making it clear that he was expected, as Home Secretary, to agree the whole mass of warrants that came before him.8 As the table above shows, a high number of warrants – which grew substantially in the wake of 9/11 – are being authorised and modified. From 1 January 2005 to 31 March 2006, the Home Secretary and other authorised individuals issued 2,243 intercept warrants and a further 553 warrants continued in force from previous years (for Scotland, the relevant figures are 164 and 43).9 No figures are given for the considerable number of warrants issued by the Foreign Secretary (who has charge of GCHQ and the Secret Intelligence Service, commonly known as MI6) and the Northern Ireland Secretary; warrants issued by the Foreign Secretary apply to communications from and to the UK.10 Very little is known about the warranting of external intercept.

Under sections 57, 59 and 65, RIPA also established an Interception of Communications Commissioner, an Intelligence Services Commissioner and an Investigatory Powers Tribunal to ensure that the intercept and investigative processes abide by the law. (Section 16 established an Investigatory Powers Commissioner for Northern Ireland.) The Commissioners’ reports are thin and generally uninformative – though the Interception Commissioner Sir Swinton Thomas’s latest report in February was noticeably more open in response to complaints that his previous reports have been ‘over-secretive’. The Tribunal, set up to hear and investigate complaints, has yet to use its powers to quash warrants and award compensation.

### The informed consensus

As we say above, there is an informed consensus – among which there are those who are known to be sympathetic to the executive’s position on security matters – for lifting the ban. The Joint Committee on Human Rights (JCHR) – Parliament’s own committee of MPs and peers who are charged with safeguarding human rights - reported in August 2004 that it had found ‘overwhelming support’ for lifting the ban.11 A formidable list of those charged by the government with reviewing counter terrorism legislation have recommended lifting the ban: Lord Lloyd, in his 1996 review of terrorist legislation;12 the Newton Committee review of the Anti-Terrorism, Crime and Security Act 2001;13 and Lord Carlile of Berriew, the official reviewer of counter terrorism legislation, in successive reports.14 In evidence to the Joint Committee, Lord Carlile said ‘I think it [the ban] is a nonsense.’15 Lord Newton supposed that the obstacle to lifting the ban was ‘in the minds of people who oppose it...I find it virtually impossible to understand...why there should be a complete ban on the use of evidence of this kind’, adding, ‘there was not a single member of ... the [Newton] Committee who was not of the view that it was sensible to relax this ban’.16 The most notable informed authority who is implacably opposed to lifting the ban is Sir Swinton Thomas, the retiring Interception of Communications Commissioner, who reiterates his objections in his report on intercepts from 2005-06 published in February 2007.17

Lord Carlile and Lord Newton believed that their view was
shared by many in the intelligence community, ‘apart from possibly GCHQ...there is a general view that GCHQ does not agree’, as Lord Carlile (rightly) told the JCHR, ‘but everybody else seems to agree, the police and MI5, that intercept evidence should be used in courts.’ Lord Newton spoke of ‘fairly clear indications that there was a division of opinion even amongst the intelligence agencies’.18 (Both Sir Ian Blair, the Metropolitan Police Commissioner, and Andy Hayman, the Met’s counter terrorism coordinator, have expressed the view that intercept evidence should be admissible, Hayman adding that ‘it does make us look a little bit foolish that everybody else in the world is using it to good effect.’)19

The legal profession is profoundly unhappy about the inability to use intercept evidence in court, with the Bar Council, the Law Society and JUSTICE at the fore. Both Ken Macdonald and Sir David Calvert-Smith QC, the current and former Director of Public Prosecutions, have spoken out on the value of using intercept evidence. Ken Macdonald went to the heart of the matter in the Law Society Gazette, ‘The sooner we can use intercept evidence, the sooner we can stop talking about secret courts and detention without charge.’

The JCHR’s own conclusion was that ‘the case for relaxing the absolute ban on the use of intercept evidence is overwhelming’; the ban was ‘a disproportionate and unsophisticated response to the legitimate aim of protecting intelligence sources and methods’. The Committee also raised a widely shared feeling that it was possibly a symptom ‘of an over-protective approach to information which originates from intelligence material.’20 The Home Affairs Committee on detention powers in 2006 reported ‘universal support’ for the use of intercept evidence in court and found that the Home Office had not produced ‘convincing evidence that the difficulties were insuperable: they have presumably been tackled in other jurisdictions.’21

**The value of intercept evidence**

Equally, official policy makers, the law enforcement agencies and the Interception Commissioner agree that intercept evidence is an ‘effective’, ‘essential’, ‘crucial’ and even ‘indispensable’ tool in the detection and prevention of terrorism and serious crime. From the previously mentioned privy councilor review (see In 8) for the then Prime Minister, Harold Macmillan, in 1957 to a government consultation paper in 1999, official reports have stressed the significance of intercepted communications in a fast-moving world of organised crime, international drug trafficking and terrorism. In the 1999 consultation paper, the government stated that, ‘Interception represents an indispensable means of gathering intelligence against the most sophisticated and ruthless criminals’.22 The Interception Commissioner’s report of February 2007 states that intelligence from intercept has been ‘crucial’ to the prevention of recent ‘serious prospective terrorist and criminal attacks’.23

Yet at the same time, the ban on its use in court severely restricts the value of intercept intelligence and is used to justify serious exceptions to due process and the right to a fair trial. Lord Lloyd, as the official reviewer of terrorism legislation, put the issue starkly in his 1996 report:

One of the themes that has persisted throughout [this] Inquiry is the difficulty of obtaining evidence on which to charge and convict terrorists, particularly those that plan and direct terrorist activities without taking part in their actual execution. This has proved to be a serious weakness in the anti-terrorist effort, especially in Northern Ireland. In many cases the leaders of the paramilitary organisations may be well known enough to the police, but there is insufficient evidence to convict them.24

Intelligence sources have indicated to us that it is to be expected that the police and prosecuting authorities are in favour of relaxing the ban, since the use of intercept is most likely to be of assistance in criminal cases, less so in terrorism cases.25 The latest intelligence review, reported to the House of Commons by Charles Clarke, the then Home Secretary on 26 January 2005, found that the use of intercept evidence would result in a modest increase in the conviction of serious criminals, but not of terrorists, and would come with ‘serious risks to the continual effectiveness’ of the intelligence agencies.26 Yet Lord Lloyd estimated in his inquiry into terrorism legislation that the use of intercept evidence would have allowed a prosecution to be brought in at least 20 cases.27

**Justifying the ban**

Lord Lloyd of Berwick, presenting his Private Members Bill for debate in the House of Lords in November 2005, said that for the intelligence services the thought of intercept evidence being used in court ‘makes shivers run down their spines.’28 And it is the objections of the intelligence services, and primarily GCHQ, that have prevented its use.

The overwhelming objection on the part of intelligence services to lifting the ban is that allowing such evidence would seriously compromise their interception capacities – an argument that was put with great force by the Labour peer, Baroness Ramsay of Cartvale, a former MI6 official, in the debate on Lord Lloyd’s bill. Her argument was that the domain of intercept was wider and more complex than most people, including those who were the target of intercept operations, could possibly imagine – ‘again and again,’ she said, suspects wrongly assumed that the means by which they communicated were secure:

The slightest revelation of interception risks blowing for ever the techniques involved and in some cases putting at risk human agents. It not only means the end of that particular operation but, by extension,
others which will be surmised to be in place on similar types of targets.

The very sophistication and scope of British expertise in interception rendered it ‘extremely vulnerable’, if revealed or ‘even hinted at,’ especially where material was encoded or encrypted involving very sensitive technical means and/or human agents. The loss of access in such cases was usually permanent:

A straightforward police tap on home national territory would likely have little to lose in terms of giving away techniques or endangering sensitive sources and it is that kind of material alone which some other countries permit to be used in court. [In countries] where more sophisticated techniques are employed by agencies other than the straightforward law enforcement agencies, it is only the more routine product of the law enforcement agencies’ that are produced in court.29

Intelligence sources support what Lady Ramsay had to say. GCHQ is absolutely opposed to allowing the results of its sensitive technological capacities even to be considered for use in court, arguing that the very knowledge of what it can and cannot achieve would assist terrorists. One source pointed out that terrorist rings even publish internet manuals on counter terrorist capacities. ‘People don’t realise how fragile this material is,’ said one source. ‘They just cannot keep their mouths shut.’

This person gave as an example the leak of information to the New York Times in the 1990s that the security forces were able to listen in on Osama bin Laden’s satellite phone conversations; ‘and he has never used a mobile phone since’. They also reinforce her statement that material from more sophisticated intercept is not used in court in other countries, like Australia and the United States, which do use the material from law enforcement agencies. ‘The US National Security Agency would not dream of admitting to court what material they hold. The French are the same.’ These sources stress first the difficulty of ‘disentangling’ intelligence and police material, and express doubts about the security of admitting to judges, let alone defence lawyers, sensitive material through the public interest immunity (PII) certificate process. In their view lawyers would also inevitably argue in the discovery process that it was not lawful to discriminate between one ‘secret’ and another and may well embark on ‘fishing expeditions’.

The second main set of objections to allowing the use of intercept evidence in court relate to the sheer volume of material that is collected and the demands of translating, transcribing and ordering it for use as evidence. These difficulties are not insuperable, as our sources admit, but they suggest not unreasonably that the government would be reluctant to make the additional resources required fully available to the agencies.

**Lifting the ban**

There is a circular dimension to the main argument that the intelligence community raises against the use of intercept evidence in court. Those involved in terrorism (and to a lesser degree perhaps) in serious crime are already fully aware of the possibility that their communications are liable to be intercepted. The very existence of the counter-interception manuals on the internet proclaims this; so too does their deliberately opaque modus operandi. But they are still normally obliged to make use of telecommunication networks when developing their conspiracies, especially when their activities are international in scope.31 JUSTICE additionally argues that the fear that terrorists and other serious criminals might learn compromising information on interception through disclosure in UK courts is undermined when one considers the international nature of modern terrorism and serious organised crime.32

Further, those who are opposed to the use of intercept evidence exaggerate the dangers inherent in the PII process and underestimate the ability of its safeguards to protect significant interception capabilities from being revealed in court proceedings. Only the prosecution can apply to introduce evidence, the defence cannot do so. There would be no access to intercept evidence unless the prosecution has applied and the judge has agreed. It would always be open to the Secretary of State to issue a PII certificate; and the PII process is quite capable of preventing details of covert surveillance techniques and the identity or existence of informants being disclosed to defendants, as has been shown in serious criminal trials.33 Under the principle of ‘equality of arms’, it is true, the prosecution is under a duty to disclose to the defence any material that might be of assistance to an accused person. But the Criminal Procedure and Investigations Act 1996 prohibits the court from disclosing any material that is not in the public interest. As JUSTICE argues, it is in our view inconceivable that a court would ever conclude that the interests of justice required details of surveillance or interception capabilities to be disclosed. Even if it were to do so, however, it would still be open to the Crown to withdraw the prosecution and thereby prevent the sensitive material from being disclosed to the defendant. [our emphasis]34

It is plainly the case that allowing intercept evidence would place an additional logistical burden upon the intelligence and law enforcement agencies, as our sources have argued. But equally plainly, it is not ‘insuperable’, as they admit; and certainly other common law jurisdictions surveyed by JUSTICE have met and continue to shoulder this burden. As for ‘fishing expeditions’, the courts and prosecutors are quite able to see off such attempts.
Evidence for Change | Lifting the ban on intercept evidence in court

Conclusion
The ‘shadow’ system of criminal justice that we analyse in The Rules of the Game, under which accused people may be detained without charge and denied both a lawyer of their own choosing and the opportunity to hear the evidence against them, subverts long-standing principles of British justice. The British criminal justice system is founded on the principles of fair trial and due process while seeking to establish whether accused people are guilty or innocent. It is incumbent on the authorities to restore that system, even under the strains to which international terrorism subjects it. Indeed, the fairer British justice is and is shown to be, the stronger will be the country’s defences against terrorism.

Public interest immunity has been devised and developed to strike a balance between an accused person’s right to a fair trial and the need to protect the public interest against the disclosure of damaging information. It is our view that PII provides sufficient safeguards against the disclosure of intercept information that might benefit terrorists and other serious criminals. The use of intercept evidence is not a magic bullet. It may well be, as we are informed, that it would have had no part to play in the cases against those terrorist suspects who were held in indefinite custody without trial. But the near absolute ban on its use in criminal cases is against the public interest: first, it means that serious criminals may be released when they should and could be prosecuted, and that terrorist suspects are detained without trial while they too might be prosecuted; secondly, it compromises the quality of British justice.

Sir Swinton Thomas, in his report on interceptions, criticises ‘misguided’ and ‘often ill-formed’, but ‘no doubt well-intentioned’, people who continue to re-open the complex problem of the ban on intercept evidence. Among them he notes are lawyers, some of whom are ‘distinguished’. But such people ‘do not have knowledge or experience of intelligence and law enforcement work’ and it would be wise to discuss the issue with those who are knowledgeable on the subject. 35

A dialogue of this kind would clearly be valuable (and it is worth noting that Lord Lloyd of Berwick, a long-standing champion of reform, has frequently investigated and ‘discussed the subject’ with ‘those who are knowledgeable’). But there is a wider issue here. The complex problem of intercept evidence has now been under discussion for more than ten years. It is agreed between all the agencies that at least some serious criminals could be convicted on such evidence who would otherwise escape justice.

The intelligence community is very largely autonomous and subject only to limited, and no doubt well-intentioned, oversight. It is on their advice that the government has failed to act. In introducing his Private Member’s Bill in 2005, Lord Lloyd argued that Parliament should have the chance ‘to investigate and to test that advice’:

The security services might even be persuaded that their fears are groundless, but whether they are or not, I do not believe that it is a matter that should be decided on their mere say-so. 36

Notes
2. JUSTICE has published details of the use of intercept evidence in court under seven common law jurisdictions in Australia, Canada, Hong Kong, Ireland, New Zealand, South Africa and the USA, in its valuable paper, Intercept evidence: Lifting the Ban, October 2006
4. news.bbc.co.uk/1/hi/uk/politics/336430.stm
5. JUSTICE, Intercept evidence: Lifting the Ban, October 2006, p. 3.
10. The practice of withholding these data follows the advice of the report of the Privy Councilor Review Committee, Anti-terrorism, Crime and Security Act 2001 Review, HC 100, 2003-04, in December 2003, which warned in para 121 that the disclosure even of the extent of such intercepts would aid the operations of agencies hostile to the state.
15. JCHR, op cit, 16 June 2004, Q22.
18. JCHR, op cit, 16 June 2004, Q22, Q31.
20. JCHR, op cit, para. 56.
25. Unattributable briefings.
27. Lord Lloyd of Berwick, Inquiry into Legislation against Terrorism, 30 October 1996 (Cm 3420), vol 1, p.35
30. Unattributable briefings.
31. See for example the 1999 Home Office consultation paper, Interception of Communications in the United Kingdom, op cit, para 1.3., and the 1996 Lloyd report, Inquiry into Legislation against Terrorism, para 7.17.
32. JUSTICE, op cit, para 55, p.25.
33. JUSTICE, op cit, para 56, p.25
34. JUSTICE, op cit, para 60, p.27.
36. HL Debates, 18 November 2005, col 1304.

Democratic Audit
is a research organisation at the Human Rights Centre, University of Essex.