Review of International Studies (2009), 35, 943–955 Copyright © *British International Studies Association*
doi:10.1017/S0260210509990374

Changing the rules of the game: some necessary legal reforms to United Kingdom intelligence

IAN LEIGH

Abstract. This article argues that there is a need to modernise the law governing accountability of the UK security and intelligence agencies following changes in their work in the last decade. Since 9/11 the agencies have come increasingly into the spotlight, especially because of the adoption of controversial counter-terrorism policies by the government (in particular forms of executive detention) and by its international partners, notably the US. The article discusses the options for reform in three specific areas: the use in legal proceedings of evidence obtained by interception of communications; with regard to the increased importance and scle of collaboration with overseas agencies; and to safeguard the political independence of the agencies in the light of their substantially higher public profile. In each it is argued that protection of human rights and the need for public accountability requires a new balance to be struck with the imperatives of national security.

Introduction

We have been told repeatedly since 9/11 that there is a need to re-think the balance between security and civil liberties. Although there are grounds for scepticism about whether the current crisis is so unprecedented that it requires a new paradigm, it is nevertheless undeniable that the balance has now been profoundly re-thought. There have already been already sweeping new measures in Anti-Terrorism Crime and Security Act 2001, the Terrorism Act 2005, the Prevention of Terrorism Act 2006 and the Counter-Terrorism Act 2008. What has not happened since 2001 – and is now long overdue – has been a corresponding review of accountability for security and intelligence. This is regrettable since it is axiomatic that with greater powers and funding should come enhanced scrutiny and accountability. There are many questions that a review with that focus might consider. Necessarily this article concentrates on just three aspects that seem to be pressing and that have come to prominence since 9/11. In turn these are: the use of intercept evidence, the challenges of internationalisation, and the increased risk of politicising intelligence.

The use of intercept evidence

One effect of the Global War on Terror has been to revive what is for the United Kingdom a familiar debate about the respective merits of legal and militarised

responses to terrorism. One aspect is the controversy over whether prosecution is a better option than disruption of terrorist networks and detention. Ministers have repeatedly stated that executive measures, such as detention without trial[1] and control orders,[2] are justified because information in the hands of the security and intelligence agencies cannot satisfy the criminal standard of proof beyond reasonable doubt, or could not be given in evidence without compromising sensitive sources. In this context the potential use of material obtained by interception of communications is significant because it offers the apparent prospect of using strong evidence that incriminates terrorist suspects in their own words.

The UK is unusual, however, among legal systems in currently barring evidence obtained by telephone tapping and other forms of interception of communications from being given in court. Intercept is used as a source of information in investigations and for executive measures, and to assist disruption of terrorist activities. The reason for the bar is less a concern about the invasion of privacy than the wish to maintain some element of secrecy concerning the procedures. However, there are some unjustifiable anomalies – for example, evidence obtained by bugging can be given and the ban does not apply to all courts and tribunals. A notable exception is the Special Immigration Appeals Commission where intercept evidence may be given in closed session.[3]

A debate has been raging inconclusively within government departments for several years about removing the ban on evidential use of intercepted material.[4] The apparent reason for failure to agree has been continuing concerns over the scope of disclosure likely to be ordered by the courts and in particular that this cannot be predicted in advance, with the risk that confidential sources might therefore be compromised. (Official arguments never seem to address why these possibilities are acceptable in the case of bugging evidence but not intercept). A Bill to remove the bar on interception evidence for terrorist offences was introduced by Lord Lloyd of Berwick (a former Interceptions Commissioner) in 2006/7.[5] In a careful comparative review in 2006 Justice described the ban as 'archaic, unnecessary and counter-productive'.[6] In 2008 a Privy Counsellors' review, chaired by Sir John Chilcot, came out cautiously in favour of allowing such evidence provided a legal regime sufficiently protective of national security could be constructed.[7]

A human rights lawyer is bound to remark that after paying lip-service to the principle of a fair trial, the Chilcot report treated human rights concerns that might result in disclosure as a form of 'risk' to be minimised at every point. As a result

[1] Anti-Terrorism Crime and Security Act 2001, Pt. IV.
[2] Prevention of Terrorism Act 2005.
[3] Exceptions also apply for closed proceedings of the Proscribed Organisations Appeals Commission and concerning Control Orders under the Prevention of Terrorism Act 2005. The government has proposed further exceptions for closed proceedings in appeals against Treasury freezing orders and Coroner's courts: *Privy Council Review of Intercept as Evidence*, Cm.7324 (2008), paras. 20–3.
[4] Intelligence and Security Committee, *Annual Report for 2004–5*, Cm.6510 (May 2005), paras. 92–94.
[5] Interception of Communications (Admissibility of Evidence) Bill 2006/7.
[6] Justice, *Intercept Evidence: Lifting the ban* (London, 2006), at para. 168.
[7] *Privy Council Review of Intercept as Evidence*, Cm.7324 (2008). See also Joint Committee on Human Rights, *Counter-Terrorism Policy and Human Rights: 28 days, intercept and post-charge questioning*, 19th report for 2006–7, HL Paper 157; HC 394, ch. 4.

it set a series of strict tests that any legal scheme would have to satisfy before introduction of intercept evidence – all of which focus on national security interests. These include apparently sacrificing the virtues of independent decisions on prosecution (by giving control to the intercepting authority), originator control over disclosure, and a refusal to acknowledge that *exculpatory* disclosure in a fair trial (that is, of information that may assist the defence) may place justifiable additional burdens on the agencies.[8]

Although no doubt representative of the strong official evidence the inquiry received, this approach is by means convincing to a sceptical outsider. Nor was a fair-minded independent observer likely to be won over by the strategically placed passages deleted from the published report on grounds of national security. Self-evidently national security risks come in varying shades and degrees and are largely a matter of probabilities – they are least convincing of all when set forth as unwaivable absolutes. A reading of the Chilcot report leaves the impression that the authorities want to have their cake and eat it – to use intercept as evidence where it might bring an advantage but at no 'risk'.[9] This is unrealistic. Some risk that terrorists gain fractionally more information about surveillance techniques or 'trade-craft' or that overseas agencies chafe at disclosure,[10] may have to be tolerated; just as some compromise will be necessary on the principles of open justice and adversarial trial in any such regime.

The principle that: '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'[11] would involve limitations on communication between defence counsel and the defendant which will certainly be unpopular with the legal profession.[12] This, however, is an almost inevitable corollary of such a compromise. It remains to be seen, nevertheless, whether defence lawyers could be persuaded to participate on this basis: in Australia where a similar facility for already security clearance exists, counsel have declined to do so. Beyond that, however, the degree of control that the agencies would evidently like over intercept – an absolute discretion to veto prosecutions, and no additional duties to retain, examine, transcribe intercepted material – are unacceptable on human rights grounds. The jurisprudence on Article 6 of the European Convention stresses the importance of access to unused material that may be exculpatory and that *judges* should have the final decision over disclosure.

The Chilcot report is less certain than a number of commentators that use of intercept will bring a clear advantage in allowing for prosecution of terrorist cases previously unlikely to succeed. It points out that a review of nine recent control order cases concluded that the availability of using intercept evidence in court would have made no difference (in allowing a prosecution to be brought).[13] In four cases this was because it would not have been of evidential value against the

[8] See the 'Requirements for Intercept as Evidence to be Operationally Workable': Chilcot, para. 91.
[9] At para. 90 the Chilcot report states: 'We have concluded that *any* material risk to the strategic capability of the UK's intelligence agencies would be unacceptable.' (emphasis added).
[10] This is a dubious argument in any event in view of use of intercept evidence in partner countries.
[11] Chilcot, para. 91.
[12] For a detailed and critical study of special advocates see C. Forcese and L. Waldman, *Seeking Justice in an Unfair Process: Lessons from Canada, the United Kingdom, and New Zealand on the Use of 'Special Advocates' in National Security Proceedings* (Ottawa, 2007).
[13] Ibid., para. 58.

defendants and in the remainder because national security concerns would have prevailed and militated against bringing a prosecution. Without knowing all the details it is difficult to discuss these cases; nevertheless, the conclusion is puzzling. Firstly, intercept evidence *is admissible in control order proceedings* but under special circumstances. Moreover, the fair trial standards that the courts have imposed under control order procedures using the Human Rights Act and Article 6 of European Convention on Human Rights (the right to a fair trial) already go some way to equating them to a criminal trial under circumscribed rules.[14] Secondly, few would argue that intercept should be used under the current adversarial rules in a criminal trial – and yet for the purpose of the comparison the review appears to have assumed that this would be the case. The decision had already been taken in the five cases mentioned to apply for a control order – evidently national security concerns had not outweighed *that* decision. It is unclear why a prosecution under specially protective rules should be seen so very differently. Without further explanation therefore it is difficult to accept the conclusion that the availability of intercept evidence in terrorist trials would not allow the disastrous policy of executive measures to be re-thought. Moreover, so far we have considered only half the picture.

A second reason for allowing judicial consideration of intercept evidence is that it would provide a measure of accountability over the use of interception that is simply lacking from the current regime. The UK decided to implement the 1984 ruling of the European Court of Human Rights that the then regime for telephone tapping violated the right to respect for private life, home and correspondence (Article 8 of the European Convention on Human Rights) in a minimal fashion. Unlike virtually all our allies in the UK it is a minister rather than a judge who issues warrants for interception. Although under the Regulation of Investigatory Powers Act 2000 the system is checked by a judicial commissioner and there exists a right to complain to a tribunal, the circumscribed statutory standard that these bodies are required to work to means that they are ineffective safeguards. The closer scrutiny that the authorisation of interception would inevitably receive if there were a realistic possibility of challenge in court could only be beneficial.

The most powerful reason for use of intercept in criminal proceedings, however, is that it would avoid the severe damage to human rights, democratic values and national reputation that the alternatives (detention without trial[15] and control orders)[16] have wrought.[17] As the Newton Committee concluded: 'Terrorists are criminals, and therefore ordinary criminal justice and security provisions should, so far as possible, continue to be the preferred way of countering terrorism.'[18] Nor is this just a balance of incommensurables with 'airy fairy' liberal values on the one side and hard-edged security risks on the other. By using executive measures that violate the rule of law not only has the government unintentionally done the

[14] See especially *Secretary of State for the Home Department v MB* [2007] UKHL 46; *SSHD v MB* [2006] EWCA Civ 1140; [2006] 3 W.L.R. 839.
[15] Anti-Terrorism Crime and Security Act 2001, Pt. IV.
[16] Prevention of Terrorism Act 2005.
[17] D. Bonner, *Executive Measures, Terrorism and National Security* (Aldershot: Ashgate, 2007); I. Leigh and R. Masterman, *Making Rights Real: the Human Rights Act in its First Decade* (Oxford: Oxford University Press, 2008), ch. 8.
[18] Privy Counsellors Review Committee, *Anti-Terrorism Crime and Security Act 2001 Review*, 18 December 2003.

bidding of *Al-Qaeda* in destroying cherished values, it has also created a sense of grievance that feeds into the radicalisation of young British Muslims.[19] Any realistic assessment of security risk arising from the alternatives of dealing with terrorism by criminal process or executive measures would have to weigh that damage in the balance also. As we pass the 8th anniversary of 9/11 the danger of long-term damage to democratic values from the response to the dangers of terrorism grows ever-more concrete. Now is the time to regularise how we approach the challenge by bringing it within the criminal justice system.

A clearer framework for international co-operation

Since 9/11 there is evidence of increased multi-lateral and bi-lateral co-operation in the 'War on Terror' with states that are not traditional allies, for example with Asian and Middle Eastern agencies.[20] Attempts to combat the trans-national threats of large-scale organised crime, proliferation of nuclear, biological and chemical weapons and international terrorism are the causes. The scale of these liaison arrangements (though not the specific countries involved) is a matter of official record in some cases: in 2007 the Australian Security Intelligence Organisation had 306 liaison partners in 120 countries,[21] in 2002 Canadian Security Intelligence Service had 230 arrangement with 130 countries. Comparable figures have been reported for the UK agencies.

The forms of collaboration vary from the long-term institutional and technical integration of SIGINT within the UKUSA and ECHELON systems to ad hoc bi-lateral exchanges of specific intelligence between the agencies of adversary states under conditions of deep mutual distrust.

Whatever the form, intelligence co-operation is based on quid pro quo. As the McDonald Commission put it in Canada, writing in 1981 '[T] he notion of reciprocity is [. . .] central to successful liaison arrangements with foreign agencies'.[22] It enables states with different geographical access, technical expertise, human sources, linguistic or cultural expertise to exchange and pool information and sometimes resources. There are dangers as well as benefits: of dependency, a lack of fit of strategic or foreign policy objectives, of penetration and so on. Recent US experience, both leading up to 9/11 and prior to the invasion of Iraq, illustrates a number of these points.[23]

The legal footprint of these arrangements may include: sharing of intercepted communications material for use in legal proceedings in other states; and amendments to extradition law to allow the speedy transfer of terrorist suspects

[19] A. Blick, T. Choudhury, S. Weir, *The Rules of the Game: Terrorism, Community and Human Rights* (York: Rowntree Trust, 2006).
[20] S. Lander, 'International Intelligence Co-operation: An inside perspective', *Cambridge Review of International Affairs*, 17:3 (2004), pp. 481–93.
[21] Australian Security Intelligence Organisation, *Annual Report to Parliament 2006–7* (Canberra, 2007), p. 4.
[22] Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Freedom and Security Under the Law*, Second Report, vol. 1 (Ottawa, 1981), p. 632.
[23] J. Sims, 'Foreign Liaison: Devils, Deals and Details', *J. of Intelligence and CounterIntelligence*, 19:2 (2006), pp. 195–217.

(for example, under the European Arrest Warrant). There is also the question of extraordinary rendition, that is, the removal of non-citizens to another state otherwise than through lawful deportation or extradition which may involve the co-operation of the state in whose territory a suspect is seized, of other states through whose airspace the suspect is transported and of those where he is taken for questioning.

While the need for increased networking between the agencies of different countries is undeniable there are also some clear risks. These include the possibility of compromising domestic standards of constitutionalism, legality and propriety through unregulated co-operation. At worse, co-operative arrangements may be consciously used to circumvent domestic legal controls on the obtaining of information or for protection of privacy. Moreover, there is the question of transparency – decisions may be taken that profoundly affect an individual's rights on the basis of information that is not traceable to an agency in another country and without adequate safeguards as to its accuracy or how it was collected. There can also be strong incentives for the agency that receives such information not to inquire too closely into how it was gathered – lack of curiosity may even be the price of continuing to receive intelligence from overseas partner agencies. It is therefore essential that international co-operation of intelligence services should be properly authorised and subject to minimum safeguards.

Under the current legal framework only some of these issues are addressed. Courts are likely to intervene in only the most egregious of cases over which they have jurisdiction (for example, by aborting a trial in the UK following rendition),[24] but are relatively powerless otherwise (as demonstrated in the Al-Rawi case below). The procedure for political approval of co-operation is opaque at best. Unlike some of its partner countries, UK law does not stipulate ministerial approval, require agreements to be shown to an outside review body, or protect the interest of British people expressly under such arrangements. The Intelligence and Security Committee's investigation into renditions has shown the limits of parliamentary oversight – it begins and ends with the UK end of the exchange. Parliamentary attempts to gain information about alleged CIA over-flights of UK territory, and the use of UK airports or overseas dependencies (Diego Garcia in particular) for rendition flights have likewise produced mixed results.[25] Arguably there is a legal obligation to inquire into credible allegations of UK involvement.[26]

What should happen ideally to strengthen accountability concerning co-operation? Parliament may be able to aid accountability by creating a legal framework in which co-operation between agencies is only permissible according to principles established by law and where authorised or supervised by applicable

[24] *R v Mullen* [1999] 2 Cr App R 143. See also *R v Horseferry Magistrates Court, ex p. Bennett* [1994] 1 AC 42.

[25] See the Foreign Secretary's statement HC Debs. Vol. 472, cols. 547 ff, 21 February 2008; Reprieve, submission to the Foreign Affairs Select Committee, *Enforced Disappearance, Illegal Interstate Transfer and Other Human Rights Abuses Involving the UK Overseas Territories*.

[26] Under the European Convention on Human Rights (see *Ribitsch v Austria*, European Court of Human Rights, 4 December 1995 and *Aksoy v Turkey*, European Court of Human Rights, 18 December 1996; under the UN Convention Against Torture, Arts.12 and 13. And see European Commission for Democracy Through Law (Venice Commission), *Opinion on the International Legal Obligations of Council of Europe Member States In Respect of Secret Detention Facilities and Interstate Transport of Prisoners*, 17 March 2006, Opinion no. 363/2005 {http://www.venice.coe.int/docs/2006/CDL-AD(2006)009-e.asp?PrintVersion=True&L=E}.

parliamentary, or expert control bodies. In general, co-operation with foreign agencies should only take place in accordance with arrangements approved by democratically accountable politicians, usually the executive.[27] In the UK the 1989 and 1994 legislation should be amended to incorporate this safeguard. Apart from the democratic reasons for insisting upon this safeguard this should also aid transparency since it makes plausible deniability by governments harder. Both the supply and receipt of data should be required by law to be regulated by agreements in writing made by the proper authorities – a good example being the Netherlands Intelligence Services Act 2002.[28] These should be submitted to parliamentary or expert oversight bodies- for example the Canadian Security Intelligence Service Act, section 17(2) requires that the Security Intelligence Review Committee be given copies of all CSIS agreements with foreign governments and international organisations. Conditions should be attached to intelligence transferred to safeguard human rights.

The cases of the businessmen resident in Britain Al-Rawi and el-Banna have highlighted the risks that information given by UK agencies to partner agencies may lead to significant human rights abuses. After their arrest in Gambia they were taken in 2005 via Afghanistan to Guantanamo Bay. In its *Renditions* report the UK Intelligence and Security Committee concluded that conditions imposed on information given by the Security Service (MI5) and the Secret Intelligence Service (MI6) to the CIA had been ignored by the latter agency.[29] This episode also demonstrates the relative impenetrability of intelligence diplomacy to legal scrutiny, as an attempt to force the Foreign Secretary to intervene on their behalf failed.[30] The Court of Appeal found that there was no such duty in the case of non-citizens and that the Foreign Secretary's refusal was not contrary to the European Convention on Human Rights. Indirectly, however, the proceedings did contribute to the Foreign Secretary's later decision to make representations to the US authorities (leading to Al-Rawi's release from Guantanamo in April 2007 and the clearance for release of el-Banna).

Legislation should contain clear safeguards against the avoidance of the controls that apply in domestic law through co-operation with foreign agencies. German legislation, for example, contains a provision making clear that in the decision to supply information the foreign concerns of the Federal Republic of Germany or the pre-eminent interests of the affected private persons deserve to be protected must take priority and that all information supplied in this way must be recorded. Moreover it is transferred subject to limited purposes.[31] These German

[27] See, for example, Law of the Intelligence and Security Agency of Bosnia and Herzegovina, Article 64 which requires approval from the Chair, before the Agency enters into an arrangement with intelligence and security services of other countries. (Additionally, the Minister for Foreign Affairs must be consulted before an arrangement is entered with an Institution of a foreign State, an international organisation of states or an institution thereof.). The Chair is obliged to inform the Intelligence Committee of all such arrangements.

[28] See, the Dutch Intelligence and Security Services Act 2002 (De Wet op de inlichtingen- en veiligheidsdiensten) Article 36(1)(d), 40(1) and 42.

[29] Intelligence and Security Committee, *Rendition*, Cm.7171 (July 2007), paras. 111–47.

[30] *R (Al Rawi and others) v Secretary of State for Foreign and Commonwealth Affairs and Secretary of State for the Home Department (United Nations High Commissioner for Refugees intervening) [2006] EWCA Civ 1279*.

[31] *Bundesverfassungsschutzgesetz* (BVErfSchG), Germany, November 2002, Art. 19 (*Unofficial translation*).

provisions are important safeguards – lacking in the legislation of many states – but arguably even these do not go far enough.

Information should only be disclosed to foreign security and intelligence agencies or to an international agency if they undertake to hold and use it subject to the same controls that apply in domestic law to the agency which is disclosing it (in addition to the laws that apply to the agency receiving it). Limits should be placed on the type of intelligence which can be transferred and there should be a requirement to check the reliability and accuracy of the intelligence, before it is transferred.[32]

A similar duty should apply for a receiving agency, to check reliability and accuracy when information is received from another state. Despite the House of Lords' judgment of December 2005 in *A (No. 2)*[33] that evidence obtained by UK agencies from foreign agencies as a result of torture could not be used in legal proceedings in the United Kingdom there are some significant gaps in the existing legal protection. As Lord Hoffmann, dissenting, noted:

> [. . .] It appears to be the practice of the Security Services, in their dealings with those countries in which torture is most likely to have been used, to refrain, as a matter of diplomatic tact or a preference for not learning the truth, from inquiring into whether this was the case. It may be that in such a case the Secretary of State can say that he has no knowledge or belief that torture has taken place. But a court of law would not regard this as sufficient to rebut real suspicion and in my opinion SIAC should not do so.[34]

The majority, however, (Lords Hope, Rodger, Caswell and Brown) ruled that the evidence would only be inadmissible if Special Immigration Appeals Commission was *satisfied on the balance of probabilities* that the evidence had been obtained by torture. In practice this sets an impossibly high hurdle for a person challenging the evidence. More specific controls should be considered therefore.

In its 2007 *Report on Democratic Oversight of the Security Services in Council of Europe States* the Venice Commission has suggested that where information is received from a foreign or international agency, it should generally be held subject both to the controls applicable in the country of origin and those standards which apply under domestic law.[35] Ideally this would mean information being subject to the oversight mechanism in full in the country that receives foreign-derived intelligence. In some cases a powerful State on whose supply of intelligence other countries are dependent may be unwilling to accede to such conditions. A possible workable fall-back arrangement, may, however, be to establish a system of certification – where the oversight institution in the state supplying intelligence at least warrants that it has been collected and handled according to local standards of legality.

Conditions like these on information exchanged between agencies might go some way to addressing concerns that have now arisen in several documented cases of information supplied by an agency upon its own nationals or residents

[32] See Arar Commission, *Report of the Events Relating to Mahar Arar, Analysis and Recommendations* (Ottawa, 2006), p. 334.
[33] *A (No 2) v Secretary of State for the Home Department* [2005] UKHL 71.
[34] Para. 98.
[35] European Commission for Democracy for Law (Venice Commission), *Report on Democratic Oversight of the Security Services in Council of Europe States, Study 388/2006 (CDL_DEM 2007–016)* (June 2007), pp. 39–40.

apparently leading to their 'extraordinary rendition' – for example the Arar and Al-Rawi cases in Canada and the UK.

More generally there is also a strong democratic case for some lifting of the blanket of official silence concerning intelligence co-operation to allow a measure of outside scrutiny, especially in view of the huge resources and semi-permanent status of the UKUSA agreement. Under the existing law information about co-operation itself is heavily protected. Thus, a criminal defendant may be tried for unlawfully disclosing information about intelligence co-operation between the two countries contrary to official secrets legislation. Under the UK Official Secrets Act 1989 section 3 it is an offence for a civil servant or government contractor to make an authorised disclosure of material damaging to international relations.[36] The 1989 Act also covers (in section 6) a damaging disclosure of information relating to security, defence or international relations that has been communicated in confidence by the UK government to another state or international organisation. These provisions have been invoked several times recently because of sensitive disclosures by civil servants about co-operation- in the Katherine Gun, Derek Pasquaill and David Keogh cases.

In the first, the prosecution of Katherine Gun, a former GCHQ employee, under section 1 of the Official Secrets Act (which concerns disclosures by security and intelligence officials) was discontinued.[37] Gun had leaked to *The Observer* newspaper a memo from the NSA confirming that a 'surge' in eavesdropping on member states of the UN Security Council had begun, prior to a key Security Council vote on Iraq. In the second, proceedings against Derek Pasquaill a Foreign Office official who had leaked documents concerning the UK government's policy of engagement towards Muslim groups and concerning extraordinary rendition were dropped in January 2008. According to news reports prosecutors apparently decided that internal Foreign Office documents undermined the claim that the disclosures were damaging.[38] Both of those prosecutions were dropped at a late stage but in a third case a Ministry of Defence official, David Keogh was convicted in May 2007 and sentenced to six months' imprisonment for passing a memo summarising a discussion held between Tony Blair and George Bush in Washington in April 2004 concerning Iraq to a researcher working for a backbench Labour MP.[39]

The converse situation to liability under the Official Secrets Act is where a litigant seeks information about co-operation under freedom of information or privacy legislation (for example, the Freedom of Information Act 2000). In both situations – and particularly in Western countries with longstanding co-operative arrangements for signals intelligence – in effect a protective wall of statutory duties

[36] Note that in the UK the government had originally proposed no damage requirement should apply to disclosures of information received from foreign governments or international organisations because of the wider damage to the UK's standing in the international community that such disclosures would cause: *Reform of Section 2 of the Official Secrets Act 1911*, Cm 408 (1988), para. 51.

[37] Katherine Gun, 'Ex-GCHQ Woman Cleared Over Leak', BBC News (13 November 2003), {http://news.bbc.co.uk/2/hi/uk_news/3268113.stm}.

[38] '"Brave" Official Praised for Leak', BBC News (8 January 2008), {http://news.bbc.co.uk/2/hi/uk_news/7179247.stm}. 'Official Cleared in Secrets Case', BBC News (9 January 2008), {http://news.bbc.co.uk/2/hi/uk_news/7178785.stm}.

[39] 'When Should a Secret Not be a Secret?', BBC News (10 May 2007), {http://news.bbc.co.uk/2/hi/uk_news/6639947.stm}.

and exemptions has been erected in each country to enable co-operation to continue away from public scrutiny. Despite the clear rationale for freedom of information exceptions like these they also have the collateral effect of largely rendering legally invisible exchanges of information between the security and intelligence institutions of different countries. Only where some form of open action is envisaged on the basis of the information exchanged is there a risk of disclosure.

Ostensibly, the purpose of such exemptions is the sensibilities of the partner agency in an overseas country: the fear of the consequences if co-operation were to be withdrawn is regularly invoked as official justification. Statements referring to the adverse impact on efforts to safeguard national security if foreign-derived intelligence were to dry up can be found in official documents and evidence given in litigation in several countries. However, the very fact that such similar statements are tendered in partner countries (each invoking the threat of the other withdrawing co-operation) raises a suspicion that the alleged sensitivities of the other state may be no more than a convenient proxy for a more generalised unwillingness to allow scrutiny of co-operation as such. Arguably there is a case for greater scepticism, both by the courts and the information commissioner over claims that disclosures will damage such co-operation.

Alasdair Roberts has argued that security of information agreements between states may give rise to 'a reasonable expectation of complete secrecy' and that they may 'deny domestic actors, including the courts, the opportunity to make their own decisions about the disclosure of information within a certain policy domain'.[40] While this is helpful in explaining the stance of some governments with regard to freedom of information legislation and litigation, taken as normative propositions these statements are nonetheless contentious in a way that goes to the heart of the debate.[41]

The underlying question is whether such arrangements should operate in a twilight zone devoid of constitutional and legal control. The idea that secret agreements between governments should dictate the content of domestic legislation on freedom of information offends all notions of constitutionalism and democratic accountability.

Strengthening the safeguards against politicisation

Security and intelligence are perhaps now more central to the government machine than at any time since 1945. At the same time there is greater visibility – through the public use of intelligence (notoriously so in the case of the dossiers released prior to the Iraq war),[42] through public threat commentary from MI5 and interventions by officials in public discussion of the need for new counter-terrorist

[40] A. Roberts, 'Entangling Alliances: NATO's Security of Information Policy and the Entrenchment of State Security', *Cornell Int LJ*, 36 (2003), pp. 319, 355.

[41] Roberts, pp. 359–60.

[42] The government published two controversial dossiers of intelligence material in September 2002 and January 2003: P. Gill, 'The Politicization of Intelligence: Lessons from the Invasion of Iraq', in H.Born, L.Johnson and I.Leigh (eds), *Who's Watching the Spies: Establishing Intelligence Service Accountability* (Dulles VA: Potomac, 2005).

powers. With exposure comes the significant risk of politicising security and the presentation of intelligence. The current arrangements – designed for different times – give insufficient protection against 'politicisation'.

At present the only safeguards are short provisions in the 1989 and 1994 legislation (designed with the contentious notion of counter-subversion in mind) preventing the agencies from furthering the interests of any UK political party.[43] In the background, of course are the traditions of the British civil service concerning neutrality. Concrete suggestions for reform might be made in two areas – senior appointments and ministerial instructions.

Unlike the United States, there is no tradition in the United Kingdom of confirmation by the legislature of the appointment of key officials. The executive alone is responsible. Consequently, the appointments of heads of the agencies are made by Ministers (presumably advised by the head of the civil service, the Cabinet Secretary) but without reference to the ISC for example. This gap became apparent with the political controversy in May 2004 surrounding the appointment of John Scarlett as 'C' (the head of SIS);[44] Scarlett was the Chairman of the Joint Intelligence Committee (JIC) and a central figure in the controversy over the public use of intelligence in the Iraq war then still under investigation by the Butler review. When it reported two months later the Butler review apparently felt that Scarlett's position had been undermined and that it was necessary to endorse his new appointment, notwithstanding its published criticisms.[45]

One safeguard is for external involvement or scrutiny of the appointment of the Director of the intelligence and security agencies. Other countries employ formal confirmation or consultation procedures, to allow the legislature to either veto or express their opinion on an appointment. There may be a constitutional requirement either that official appointments must be approved by parliament or, at least allowing them to be blocked by a parliamentary vote (for example, the practice in the US). In Belgium, the director-general is obliged to take the oath before the chairman of the Permanent Committee for Supervision of the Intelligence and Security Services before taking office.[46] In Australia, the Prime Minister must consult with the Leader of the Opposition in the House of Representatives concerning the proposed appointment.[47] The aim of such provisions is to achieve a broad political backing for the Director's appointment. In the UK the Brown government has conceded in its 2007 Green paper *The Governance of Britain* that Parliamentary scrutiny of some appointments to independent non-departmental bodies is desirable.[48] In view of the non-partisan position of the agencies heads (recognised in their statutory responsibilities) there is a case for treating them differently to other civil servants and applying this new process to them also.

[43] Security Service Act 1989, section 2(2); Intelligence Services Act 1994, sections 2(2)(b) and 4(2)(b).
[44] 'Ex-KGB man backs new MI6 Chief', BBC News (7 May), available at: {http://news.bbc.co.uk/2/hi/uk_news/politics/3689779.stm}. Political controversy also broke out in July 2009 concerning the appointment of Sir John Sawers as Scarlett's successor following publication of personal details on Lady Sawers' Facebook page: 'Miliband Defends Future MI6 Chief', BBC News (5 July 2009), {http://news.bbc.co.uk/1/hi/uk/8135070.stm}
[45] *Report of a Committee of Privy Counsellors*, 2004, para. 39.
[46] Act Governing the Supervision of the Police and Intelligence Services, 1991, Art. 17
[47] Part 3, Section 17 (3), Intelligence Service Act, Australia, 2001 (Cth).
[48] *The Governance of Britain*, Cm.7170 (July 2007), paras. 72–81.

Another area for safeguards concerns political instructions. All the UK services work under the authority of ministers but under the control of their directors. The boundaries of the distinction between 'authority' and 'control' are unclear and potentially movable. A legal requirement that certain ministerial instructions be put in writing (as exists for example, in Canada and Hungary)[49] can act as aid to accountability by preventing 'plausible deniability' and even prevent some questionable instructions from being given in the first place because to do so would involve a paper trail. An example combining protection of human rights is the Australian legislation requiring the ministers responsible for the Australian Secret Intelligence Service, and the responsible Minister in relation to the Defence Signals Directorate, to issue written instructions to the agency heads dealing with situations in which the agencies produce intelligence on Australians.[50] In addition, a requirement that ministerial instructions must be disclosed outside the agency may act a checking device. Examples can be found in Canadian law, which requires them to be given to the Review body, and Australian legislation, requiring them to be given to the Inspector-General of Intelligence and Security as soon as practicable after the direction is given.[51]

Conclusion: new game, new rules

The past decade has brought important changes to the size and funding the security and intelligence agencies, their public and legal profile, their international liaison work and their place in governmental decision-making. Increasingly, the legal structure that the agencies operate within is showing its age – despite being passed in 1989 and 1994, the legislation was really a codification of mid-20th century understandings, given a light democratic makeover. In an era of much more open and informed discussion concerning security and when the government is attempting to enlist public and judicial support against terrorism, more radical up-dating is long overdue. The age of blanket secrecy over security and intelligence is long passed. It is increasingly untenable, therefore, to cling to rules designed to insulate interception and international co-operation from public gaze.

In the case of intercept evidence the government's attachment to the outmoded exclusionary rule has led it in the direction of utilising executive measures in preference to criminal trials for some terrorist suspects. The reasons why the intercept ban has been retained are in part at least confused and illogical. What is clear, though, is the enormous damage that the consequent diversion of cases away from the criminal courts has inflicted on human rights, on the UK's international standing, and, ultimately, on its security. The case for change to the intercept evidence ban is clear, but change must genuinely balance human rights concerns, rather than trampling them under indefensible security absolutes.

[49] Canadian Security Intelligence Service Act 1984, Sections 7(1) and (2); Act on the National Security Services 1995, Hungary, s. 11.
[50] Intelligence Services Act 2001 (Australia), s. 8(1).
[51] Canadian Security Intelligence Service Act 1984, s. 6(2), and Australian Inspector-General of Intelligence and Security Act, 1986, s. 32B, respectively.

The globalisation of intelligence is increasingly rendering irrelevant the legal structures adopted by many countries in the last quarter of the 20th century to protect individuals from abuses by their agencies. In the UK's case the legislation does not adequately address even the most basic of questions concerning international intelligence co-operation, such as how and when it is authorised, still less the more complex issues about flows of information concerning individuals. There is an urgent need to democratise intelligence diplomacy and to open it to a measure of scrutiny and accountability.

The increasing visibility of security agencies, the advice that they give and the decisions based upon it gives rise also to pressures of politicisation of intelligence. Here too the existing statutory safeguards are inadequate. In a modern constitutional setting it is time to build on the traditions of neutrality and independence of the agencies with stronger legal safeguards so that public confidence can be restored.

The swathe of counter-terrorist powers enacted in the last decade cries out for equivalent changes to strengthen the framework of accountability of the security and intelligence agencies. In the three areas discussed here – the use of intercept evidence, accounting for international intelligence liaison and safeguarding against politicisation – there is now a clear need to re-balance security and democratic values.