Secrets, Spies and Whistleblowers: Freedom of Expression in the UK

by Article 19 and Liberty

SECRETS, SPIES AND WHISTLEBLOWERS

Freedom of Expression and National Security in the United Kingdom

ARTICLE 19 and Liberty

November 2000

Printed by The Guardian

ACKNOWLEDGEMENTS

This report was researched by Steven Warner, with assistance from John Wadham, Director of Liberty and Selina Chen, ARTICLE 19 Policy Researcher. It was edited by Toby Mendel, Head of ARTICLE 19 Law Programme and Ilana Cravitz, Head of Communications at ARTICLE 19. It was copyedited by Katherine Huxtable, ARTICLE 19 Press Officer and designed by Mark Jordan of The Guardian.

Liberty and ARTICLE 19 gratefully acknowledge the generous support received from the Scott Trust and the Joseph Rowntree Charitable Trust for the research, editing and publication of this report. Many thanks also to The Guardian production team.

CONTENTS

EXECUTIVE SUMMARY

This joint publication by ARTICLE 19, the Global Campaign for Free Expression and Liberty is a critical analysis of UK laws and mechanisms which ostensibly safeguard national security but which have, in practice, been used by successive governments to suppress embarrassing or controversial revelations and to undermine the public's right to know.

Freedom of expression in the UK has been described by some as "bred in the bone of common law" and the UK media are said to enjoy enviable freedom in most matters. Yet, at the same time, UK governments have a record on secrecy which few other western democracies can match. Consequently the British media's ability to function as a "watchdog" of certain areas of official activity is severely and deliberately impeded by legislation and official practice.

It is widely recognised in international law that freedom of expression is not an absolute right and can legitimately be restricted if it harms national security. However, all such exemptions must be accompanied by adequate safeguards to protect against their misuse by governments and to ensure that the balance between national security and freedom of expression is properly struck. Such safeguards are absent from the UK's legislative framework. The pattern seen in the courts has been less a careful balancing of freedom of expression and national security than judgments that damage free expression and suppress revelations of incompetence, illegality and other wrongdoing by members of the security and intelligence services and the armed forces.

The UK Government has a battery of means at its disposal to ensure that a veil of official secrecy is maintained and the activities of the Security and Intelligence Services (SIS) remain unexamined. Chief among these is the draconian Official Secrets Act (OSA), which prohibits the disclosure of a huge range of information by government employees and the media. Those breaching the OSA face imprisonment and fines.

The OSA makes it a crime for current and ex-members of the Security and Intelligence Services to reveal any security-related information, even if such information is not damaging to national security, putting the UK out of step with many other democracies. Further, in many other democratic states such as Germany and the Netherlands, publication of official secrets and information harmful to national security can be excused if it serves the public interest. No such defences for whistleblowers or the recipients and publishers of their information exist under UK law.

A raft of other mechanisms is also used in the UK to suppress information, obtain documents, compel disclosure of sources and trace and punish those responsible for disclosures of national security related information. Injunctions, production orders, confidentiality clauses and contempt of court laws are just some of the civil and criminal mechanisms at the Government's disposal. All have been invoked in recent years in the executive's readiness to seek gagging orders, fines and prison sentences for public servants and journalists who use protected information to publicise documents and allegations relating to official incompetence, illegality or wrongdoing. Other powers, such as search and seizure by police, are also used to obtain

information. In the use of injunctions as a preferred means of suppressing information, the British authorities are unfettered by the constitutional, statutory or judicial safeguards governing prior restraint in countries such as Austria, France, Sweden and the US. Nor do UK journalists enjoy the same right as their counterparts in many other European countries to protect the confidentiality of their sources.

The report identifies the alarming tendency of the UK judiciary to defer to the Government in these matters and its failure to observe the necessity to balance national security considerations against the public interest and the right to freedom of expression.

Among the recommendations we make are:

- that the Government conducts a review of all law and practice relating to national security, including ongoing prosecutions;
- introduction of mechanisms for proper democratic scrutiny of the activities of the security and intelligence services;
- establishment of a narrow definition of national security;
- specific inclusion of a substantial harm test for disclosures relating to national security offences and a public interest defence for those accused of breaching official secrecy; and
- legal protection for Security and Intelligence Services "whistleblowers".

This report further provides an analysis of how the UK Government uses the law to prevent disclosures of security-related information by government employees, the media and members of the public. The legislative framework is measured against international legal standards and found wanting. The report also analyses the role of the judiciary and its failure to subject government claims about national security to close scrutiny. It sets out the laws and mechanisms which restrict disclosure of national security-related information, and details the ways in which this matrix of civil and criminal legislation has been used by the Government in the last three years against former security service employees, members of the public, and the media.

The report also considers the Human Rights Act 1998, which incorporates the European Convention of Human Rights into domestic law, and its implications for reforming the UK regime of freedom of expression in the context of national security. The report discusses the options open for reform, and concludes with a list of fourteen recommendations that would ensure that the UK regime governing freedom of expression and national security conforms to the standards and practices befitting a modern, open and healthy democratic society.

Summary of Recommendations

Recommendation 1: The government should immediately review all national security laws for compliance with these recommendations.

Recommendation 2: All ongoing prosecutions and other legal measures, as well as any sanctions already imposed, should be reviewed for compliance with these recommendations and remedial measures taken where necessary.

Recommendation 3: All national security restrictions should be subject to a full appeal on the merits by the courts.

Recommendation 4: All national security legislation should include a clear and narrow statutory definition of national security.

Recommendation 5: Those seeking to restrict expression should bear the burden of proving that the restriction complies with these recommendations.

Recommendation 6: No restriction on expression or information should be considered legitimate unless it meets the three-part test under the European Convention.

Recommendation 7: No one should be subject to criminal penalty for disclosure of information unless that disclosure poses a real risk of substantial harm to a legitimate national security interest and there was a specific intention to cause harm of that sort.

Recommendation 8: All restrictions on expression and information should be subject to a public interest defence.

Recommendation 9: Any sanctions for breach of laws restricting expression or information should be proportionate to the offence.

Recommendation 10: A series of limitations should be imposed on the granting of injunctions to bring them into line with international standards on freedom of expression.

Recommendation 11: Journalists should not be required to reveal confidential sources or information unless this is justified by an overriding public interest.

Recommendation 12: The DA-Notice system as presently constituted should be dismantled.

Recommendation 13: The protections of the Public Interest Disclosure Act 1998 should apply to security and intelligence personnel.

Recommendation 14: The Intelligence and Security Committee should be given full Select Committee status.

Abbreviations

DA	Notice System Defence Advisory notice system
ECHR	European Convention on Human Rights
FOI	Bill Freedom of Information Bill FRU Force Research Unit
GCHQ	Government Communications Headquarters
ICCPR	International Covenant on Civil and Political Rights
MI5	Intelligence service governing security in the UK
MI6	Service governing foreign security
MoD	Ministry of Defence
OAS	Organisation of American States
OSA	Official Secrets Act
OSCE	Organisation for Security and Co-operation in Europe
PACE	Police and Criminal Evidence Act 1984
PIDA	Public Interest Disclosure Act 1998
PTA	Prevention of Terrorism Act
RIP	Regulation of Investigatory Powers Act 2000
SAS	Special Air Service
SIAC	Special Immigration Appeals Commission UN United Nations Preface

Preface

In the last few years, the issues surrounding whistleblowing, freedom of expression and national security in the UK have been attracting high levels of attention. The British government's singleminded pursuit of various ex-intelligence officials, journalists and media outlets has generated much controversy. Not since Clive Ponting was acquitted by a jury acting against the instructions of the judge,[1] and Sarah Tisdall was convicted and imprisoned in order to deter other civil servants from leaking information to the media,[2] have offences under the Official Secrets Acts been the subject of such debate. Not since Peter Wright was pursued through the civil courts of several countries for years on end – at a cost to the taxpayer of some £3 million – in a failed attempt to prevent publication of his memoirs, have injunctions enjoyed such a high media profile.[3]

The British Government "has an appalling record of attempting to classify as 'top secret' mere political embarrassment."[4] Only recently, the Government's record in this area attracted criticism from the UN Special Rapporteur on Freedom of Opinion and Expression.[5] But if the recent disclosures have substance, it is not mere embarrassment that the government has shown itself keen to avoid through its actions, but also the exposure of, and need to take action on, illegal and dangerous activities

[1] R v Ponting [1985] Crim. L.R. 318
[2] R v Tisdall (Sarah) (1984) 6 Cr.App.R.(S.) 155. Court of Appeal, Criminal Division
[3] "Troubled history of Official Secrets Act", BBC News 18 November 1998, <<news.bbc.co.uk/hi/english/uk/newsid_216000/216868.stm>>
[4] Nigel West, "Lifting the veil on [the] Security Service", Letters to the Editor, The Times, 5 June 2000
[5] Civil and Political Rights, including the Question of Freedom of Expression, Report submitted by Mr. Abid Hussein, Special Rapporteur on his visit to the United Kingdom of Great Britain and Northern Ireland to the Commission on Human Rights, E/CN.4/2000/63/Add.3, 11 February 2000

by a branch of the Secret Intelligence Services (MI6)[6] and the Force Research Unit (FRU), a disbanded branch of army intelligence.[7]

This report was commissioned by Liberty and ARTICLE 19 as a response to the increased – and increasingly oppressive – use of national security laws by the UK Government to gag and punish whistleblowers and the media. The UK legal regime currently permits no way of protecting whistleblowers who work within the Security and Intelligence Services, and instead provides a battery of legal mechanisms to punish and deter them. Rather than investigating whistleblowers' claims and making public any evidence it may have that the allegations are false, the Government has made use of these mechanisms to try and limit their dissemination. David Shayler, Richard Tomlinson, "Martin Ingrams", Nigel Wylde, Liam Clarke, Tony Geraghty, Martin Bright, Julie-Ann Davies, Ed Moloney and James Steen are currently or have recently been subject to injunctions and/or threats of imprisonment.

The UK regime governing national security and freedom of expression fails to meet internationally accepted standards of freedom of expression and compares unfavourably in this respect with other established democracies. Whereas many other countries have long had declassification and disclosure procedures which give substance to the public's right to know about their governments' activities, UK governments have to date resisted attempts to introduce effective freedom of information legislation. The draft law on freedom of information currently going through Parliament is a great deal less progressive than those published by transitional democracies such as Bulgaria and Moldova, and includes broader exemptions than those felt to be necessary in the laws of Australia, Canada, Ireland and New Zealand.[8]

One place from which to begin to understand the deficiencies of the UK regime is the lack of judicial scrutiny. In the US, the Netherlands and Germany, the courts exercise the power to examine government claims that national security is harmed.[9] In France an independent commission which has access to classified information decides whether the courts can have similar access. By contrast, the judicial standard in British courts appears to be a virtually unquestioning acceptance of the Government's claims of national security, with no body independent of the executive to hold the Government's claims to account.

Now is an apposite time to reconsider the UK regime governing freedom of expression and official secrecy. The European Convention on Human Rights has been incorporated into domestic law via the Human Rights Act 1998, which came into force in October 2000. It will fundamentally change the legal landscape. The right to freedom of expression will cease to be defined purely by common law rules, as a residual freedom occupying the space left by statutory restrictions. It will itself be established by statute – a statute, moreover, against which all others must be assessed for compatibility. This offers a rare opportunity for UK law and practice to be

---

[6] David Shayler has alleged that MI6 was involved in a plot to assassinate Colonel Muammar Gaddafi, the Libyan Head of State

[7] The pseudonymous "Martin Ingrams" has alleged that the FRU sought to destroy evidence of crimes committed by one of its informers by lighting a fire in the offices occupied by the Stevens Inquiry team

[8] Submission to the UK Government on the Freedom of Information Bill, July 1999 ARTICLE 19, Censorship News: Issue 53

[9] Sandra Coliver (ed), Secrecy and Liberty: National Security, Freedom of Expression and Access to Information, Kluwer Law, 1999, Freedom of Information: An Unrecognised Right – The Right to know and the EU, An EFJ Briefing Document <www.ifj.org/regions/europe/efj/en/eusurvey.html>

assessed for their compatibility with the requirements of the European Convention and to be reformed to provide more robust protection of freedom of expression against misuse of national security exemptions. ARTICLE 19 and Liberty present this report in the hope that its recommendations will provide a useful starting point for the discussion which must take place, and for the reform process to begin.

Liberty and ARTICLE 19, November 2000

1 International law and principles of free expression

The right to free expression is of fundamental value to society. It is a right that lies at the heart of democratic society, because it makes possible the meaningful exercise of citizens' democratic rights. For this reason, it has been described as "the touchstone of all the freedoms to which the United Nations is consecrated".[10] The guarantee of free expression is a key means of holding government to account and of protecting citizens against abuses of their rights. The press, as the conduit through which individuals can disseminate and obtain information, has a "pre-eminent role … in a State governed by the rule of law".[11]

The right to freedom of expression is enshrined in a range of international and regional treaties and instruments which bind the United Kingdom. These include Article 19 of the International Covenant on Civil and Political Rights (ICCPR), which codifies the Universal Declaration of Human Rights, and Article 10 of the European Convention on Human Rights (ECHR). Freedom of expression also enjoys recognition in the African Charter on Human and Peoples' Rights and the American Convention on Human Rights.

Article 19 of the ICCPR and Article 10 of the ECHR encompass the right both to receive and to impart information. If an individual or a journalist is prevented from making a certain piece of information public, or reporting a particular story, that infringes the individual's or journalist's right to impart information and the reader's right to receive information.

ICCPR:

Article 19(2) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print?

Article 19(3) [Freedom of expression] may … be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

a) For respect of the rights or reputations of others

b) For the protection of national security or of public order, or of public health or morals

ECHR:

Article 10: Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers?

Article 10(2) The exercise of these freedoms?may be subject to such formalities, conditions, restrictions or penalities as are prescribed by law and are necessary in a

[10] UN General Assembly Resolution 59(1), 14 December 1946, cited in written comments submitted by ARTICLE 19 in the case of Leader Publications (Pvt) Limited v Rubasinghe and Ors, 30 June 2000, S.C. (F/R) No. 362/2000

[11] Thorgeirson v Iceland, 25 June 1992, 14 EHRR 843, para.63

democratic society, in the interests of national security?[or] for preventing the disclosure of information received in confidence.

1.1 Striking the right balance: the three-part test

Ensuring the free flow of information is paramount in a democratic society, but at the same time, it is accepted that the right to free expression is not absolute and that it may legitimately be curtailed when trumped by competing considerations of sufficient weight. This is recognised in both the ICCPR and the ECHR, which allow for limited restrictions on freedom of expression. For example, it is acknowledged that expression may be restricted in certain cases where it harms the reputation of individuals. Similarly, national security considerations justify certain restrictions on freedom of expression.

However, any restriction must satisfy certain stringent criteria in order that they do not encroach upon the legitimate scope of free expression. There is a well-founded danger that governments will misuse exemptions to prevent speech for reasons other than that stated, particularly where it involves national security. It is not sufficient for a government simply to assert that national security is in issue. Rather, international and national jurisprudence, as well as the clear language of the treaties, requires that any restrictions meet the following three-part test, as set out by the ECHR and other courts:

The first requirement is that the restriction be prescribed by law. The idea of lawfulness which flows from this encompasses several distinct components. It means, first, that the restriction must be set clearly in law, for example, in the statutes enacted by Parliament, through the common law articulated by judges, in secondary legislation, or in professional rules. Second, the restriction must be articulated with sufficient precision to meet the tests of legal certainty and foreseeability; it is important for citizens and the press to be able to understand their obligations and predict when a certain disclosure is likely to be unlawful. Laws which are excessively vague or which allow for excessive discretion in their application fail to protect individuals against arbitrary interference and do not constitute adequate safeguards against abuse. They "exert an unacceptable chilling effect on freedom of expression as citizens steer well clear of the potential zone of application to avoid censure."[12]

The second criterion that a restriction on freedom of expression must meet is that it be genuinely directed towards achieving one of the legitimate aims specified in the treaties. If an individual's freedom of expression is to be curtailed in the interests of national security, the restrictions imposed must actually protect national security. Restrictions that prevent the public from learning of illegality and wrongdoing from whistleblowers in our state institutions fail this part of the test.

Even where a restriction can satisfy the first and second criteria, it will be a legitimate limitation on the right to free expression only if it is necessary in a democratic society. This criterion will be met only where the restriction fulfils a pressing social need.[13] The notion of necessity requires, in addition, the key element of proportionality.[14]

---

[12] Written comments submitted by ARTICLE 19 in the case of Leader Publications (Pvt) Limited v Rubasinghe and Ors, 30 June 2000, p.9

[13] Sunday Times v United Kingdom, 26 April 1979, No 30, 2 EHRR 245

[14] Handyside v United Kingdom, 7 December 1976, No 24, 1 EHRR 737

Where national security does require that freedom of expression be curtailed, the restrictions imposed must impair that right as little as possible, or at least not to an extent disproportionate with the importance of the legitimate aim being pursued.

These criteria establish a general presumption in favour of free expression. Free expression is the basic default position from which any departure must be justified. The exceptions in Article 10(2) must be construed narrowly.[15] Only where these criteria are fulfilled will it be legitimate to curtail the right to free expression in the name of national security. The burden of demonstrating the validity of the restriction should rest with the authorities. Moreover, claims to have satisfied the criteria for a legitimate restriction must be subject to proper independent scrutiny.[16] The judiciary has a crucial role to play in ensuring that freedom of expression is impeded no more than is strictly required in the public interest.

1.2 The Johannesburg Principles

The aim of the Johannesburg Principles[17] (see Appendix 1) is to spell out more clearly what these standards require of governments in relation to national security. Drawing on international and regional case law, the Johannesburg Principles were defined by a group of experts convened by ARTICLE 19 in October 1995. Their aim is to clarify the meaning of – and the scope of justifiable limitations upon – the right to free expression as contained in various international conventions and covenants, including the ECHR. This "fleshing out" has received positive comment from the UN Special Rapporteur for Freedom of Expression and the UN Special Rapporteur on the Independence of Judges and Lawyers.[18]

The Principles recognise that national security is a valid reason for imposing restrictions on the free flow of information.[19] However, if the presumption in favour of freedom of expression and of access to information is to be respected, the scope of the exception needs to be defined as strictly and as narrowly as possible. To this end the Principles include a clear definition of what constitutes legitimate national security interest. A restriction on the right to free expression is justified in the interests of national security only if its effect is to "protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force."[20] Moreover, the presumption in favour of freedom of expression requires governments to demonstrate that the expression will actually harm national security; the mere assertion of this by the executive will be insufficient.

The principles also state explicitly that the public's right to information must be given due weight. A state may not categorically deny access to all information related to national security, but designate in law only those specific and narrow categories of information necessary to protect legitimate national security interests (Principles 11,

---

[15] Sunday Times v United Kingdom, 1979, 2 EHRR 245
[16] Silver and Others v United Kingdom, 25 March 1983, No 61, 5 EHRR 347; Handyside v United Kingdom 7 December 1976, No 24, 1 EHRR 737
[17] The Johannesburg Principles:National Security, Freedom of Expression and Access toInformation, ARTICLE 19, Media Law and Practice Series, 1996
[18] Sandra Coliver, ?Commentary on the Johannesburg Principles,' in Sandra Coliver et al, Secrecy and Liberty: National Security, Freedom of Expression and Access to Information, Kluwer Law, 1999, pp.80-81
[19] Principle 1(c)
[20] Principle 2(a)

12). As a result, once a piece of information is in the public domain no threat to national security is posed by further disclosure, and these cannot legitimately be prevented. Such actions do not meet the legitimate aim of restricting free expression to protect national security, as the Spycatcher case established.[21]

In addition, the Principles state the widely accepted view that there is a fundamental public interest in knowing about wrongdoing and illegalities. National security cannot be used to prevent disclosures exposing illegalities or wrongdoing, no matter how embarrassing to the government.[22] There is no justification for punishing whistleblowers when they reveal information that is embarrassing or that exposes wrongdoing. This aspect of the public interest remains fundamental even when such disclosures harm national security. No person may be punished for making disclosures that damage national security if the public interest in knowing the information outweighs the harm from disclosure.[23] Whistleblowers' freedom of expression should therefore be recognised to be worthy of protection, even when legitimate national security considerations are in play.

1.3 Conclusion

Preserving free expression and the interests of national security is not just a question of finding the appropriate balance in situations where the two appear to conflict. It is also necessary that ultimately this balance should be struck by bodies, particularly the courts, that are not open to abuse by government. Those who wield executive power may act in their own political interest, rather than the broader public interest, and abuse restrictions to avoid embarrassing revelations, and the exposure of incompetence, illegality and other forms of wrongful action. As we shall see, ensuring that the procedures and mechanisms work to safeguard freedom of expression requires, among other things, a clear definition of national security that is subject to critical judicial oversight.

[21] The Observer and Guardian v. United Kingdom, (Spycatcher case), 26 November 1991, No 216, 14 EHRR 153
[22] Principle 2(b)
[23] Principle 15 and Principle 16

2 "National security": who decides? The lack of effective judicial scrutiny

2.1 National security exemptions

It is essential that restrictions on freedom of expression, including for reasons of national security, be subject to effective oversight by the courts. To fulfil this function, it is necessary for the judiciary to be able decide whether, in fact, national security is threatened. In Britain, the right to effective review is undermined by the limited scope of judicial oversight and the lack of any clear statutory guidelines for examining what national security covers.

The extent of supervision by the courts of national security restrictions is presently limited to the standard of judicial review. This is satisfied if the government can persuade the court that national security was considered as a relevant factor when the contested decision was made. Under this approach, judges do not evaluate whether the decision-maker came to a correct decision, in other words, whether national security actually does justify the restriction.[24]

The potential for misuse of national security exemptions is exacerbated by a tendency towards judicial deference in issues involving national security. For example, Richard Tomlinson, an ex-MI5 officer, was denied recourse to an employment tribunal simply on the grounds that the government would have to divulge information relating to national security.[25] Similar deference tends to prevail when the government seeks injunctions to prevent disclosures of purportedly sensitive information.[26] It has been observed that "courts in countries around the world tend to demonstrate the least independence and greatest deference to the claims of government when national security is invoked."[27] The European Court of Human Rights has tended in the past to regard a state's "margin of appreciation" – its discretion to determine for itself the compatibility of restrictions on rights with the ECHR[28] – as being widest where national security considerations are involved.[29] At the very point where domestic courts become most deferential and least inquisitive, the European Court appeared to be more willing to take governments' claims at face value.

Misuse of the legitimate national security exemption in the UK to avoid embarrassment and gag whistleblowers has been facilitated by the fact that the concept of national security is often left undefined. It is defined neither in the ECHR nor anywhere in UK legislation. National security has been described as a protean

[24] Council of Civil Service Unions v Minister for the Civil Service [1985] AC 374. Court of Appeal
[25] Philip Willan, "Renegade spy to give himself up in return for tribunal hearing" The Guardian, 3 June, 2000
[26] Laurence Lustgarten, "Freedom of Expression, Dissent, and National Security in the United Kingdom," in Sandra Coliver et al, Secrecy and Liberty: National Security, Freedom of Expression and Access to Information, Kluwer Law, 1999, pp.467-468
[27] Sandra Coliver, "Commentary on the Johannesburg Principles," in Sandra Coliver et al, Secrecy and Liberty: National Security, Freedom of Expression and Access to Information, Kluwer Law, 1999, p.13
[28] A doctrine first articulated in Handyside v United Kingdom, 7 December 1976, No 24, 1 EHRR 737
[29] Paul Mahoney and Lawrence Early, "Freedom of Expression and National Security," in Sandra Coliver et al, Secrecy and Liberty: National Security, Freedom of Expression and Access to Information, Kluwer Law, 1999, p.123

idea,[30] and an ambulatory concept[31] to be construed in light of the circumstances of each case. However the need for flexibility should not preclude both reasonable certainty of what it covers and sufficient scrutiny by others of whether in fact it is harmed.

2.2 Encouraging changes: the Special Immigration Appeals Commission (SIAC)

The European Court has indicated that national decision-makers have a margin of appreciation in matters concerning national security. The margin of appreciation is a highly contested doctrine but in any case, the Court has established that this margin of appreciation is far from infinite. In certain rulings, it has shown itself to have teeth, able to tear at the veil of national security that governments draw around their actions. In so doing, it has indicated that the ECHR requires our domestic judiciary to subject governmental claims regarding national security to a deeper and more critical scrutiny than is generally the case.

As described in section 1.1, judges too often leave the definition of national security largely in the hands of the executive, which effectively gives those with an interest in suppressing embarrassing or inconvenient information carte blanche to define national security for their own convenience. This has been recognised to be unacceptable by the European Court of Human Rights, which has held that judicial review in the UK fails to provide an effective remedy to the applicant, as required by Article 13 of the ECHR.[32] In the case of an Egyptian cleric's appeal against deportation, the Court found that the UK Government's invocation of national security concerns was unsatisfactory grounds for refusing to divulge information justifying the deportation decision. Excessive judicial deference to the executive on the definition of national security could, therefore, similarly be regarded as contrary to the ECHR.

In response to the judgment in the Chahal case above, the government established the Special Immigration Appeals Commission (SIAC) to which immigration appeals could be referred. In a recent hearing, SIAC rejected suggestions that what constitutes a danger to national security is a matter for the government to determine and not within the competence of the courts to assess, save insofar as was necessary for judicial review purposes. Rather, SIAC took the view that the Special Immigration Appeals Commission Act 1997 had conferred on it the jurisdiction to determine for itself both the meaning of a "danger to national security" and whether that definition was satisfied on the facts in issue. Whilst the views of the executive – based on privileged access to information and expertise – were to be accorded considerable weight, the ultimate assessment of whether national security was under threat was felt to be squarely within SIAC's own remit. The Home Secretary was required to prove to a high civil balance of probabilities that, on the facts of the case, the individual was a danger to national security, as defined by SIAC.

---

[30] Secretary of State for the Home Department v Shafiq Ur Rehman, 23 May 2000, No. 1999/1268/C, para.35. Court of Appeal, Civil Division

[31] <<www.dnotice.org.uk/faqs.htm>>

[32] Chahal v United Kingdom [1997] 23 EHRR 413

The Court of Appeal has confirmed that SIAC was entitled to take this approach,[33] although in its view the SIAC had erred in framing too narrow a definition of national security. Lord Woolf MR supplied a wider definition for use by SIAC in reconsidering the case. The core of this definition is that a danger to national security exists where there is at least a "real possibility" of direct or indirect "adverse repercussions" on the security of the UK.[34]

This is the closest we have yet come to a definition of national security for the purposes of UK law. It is still a wider definition than desirable, and its application is confined to the issues of terrorism and immigration. The important point for present purposes, however, is not so much the content of the definitions offered by SIAC and the Court of Appeal, but rather the fact that SIAC has unambiguously been confirmed as the arbiter of national security for cases within its jurisdiction. The judicial deference found in judicial review proceedings was rejected in favour of a full critical scrutiny of executive claims regarding national security.

SIAC is not a typical court: its three members are drawn not only from the judiciary, but also from the Immigration Appeal Tribunal and from amongst those with "experience of national security measures".[35] In confirming that SIAC did have authority to "pierce the veil" of national security, Lord Woolf MR appears to have been impressed by this unusual composition. He noted that "[w]ithout statutory intervention, this is not a role which a court readily adopts. But SIAC's membership meant that it was more appropriate for SIAC to perform this role."[36]

2.3 Conclusion

It is unclear to what extent this approach will be regarded as ?transferable? from the context of SIAC. The fact that SIAC's statutory authority to scrutinise the executive was conferred because the European Court found excessive judicial deference to be in breach of the ECHR lends substance to beliefs that such willingness to subject claims regarding national security to proper scrutiny may travel across the court system more generally. In addition, the Human Rights Act 1998 requires public authorities, including the courts, to comply with the ECHR. As such, it is able to provide courts with the requisite authority to examine the substance of executive claims to national security along the lines of the SIAC.[37]

The lack of effective and independent judicial scrutiny on national security issues undermines the right to independent review, and makes it impossible to independently ascertain what constitutes harm in the government's application of certain laws governing official secrecy. Effective scrutiny is also crucial when the Government is granted injunctions based on a claim that the disclosure of information would be prejudicial to national security.

---

[33] Secretary of State for the Home Department v Shafiq Ur Rehman, 23 May 2000, No. 1999/1268/C, Court of Appeal, Civil Division
[34] Ibid., para.39
[35] Ibid., para.11; and s. 1 Special Immigration Appeals Commission Act 1997
[36] Ibid., para.42
[37] However, it is worth noting that Article 13 ? on which the Chahal decision was based ? is not incorporated by the Human Rights Act 1998. Consequently, there must be some danger that the courts might not recognise the Act as supplying them with the requisite authority

3 Legal restrictions on public employees? freedom of expression: restricting Primary Disclosure

There are various legal mechanisms in place for policing the boundaries between free expression and national security. The Official Secrets Act 1989 (OSA) is the most important of these. It imposes various criminal penalties for unauthorised disclosures by current and former public employees as well as for non-employees (see Chapter 4). Of at least equal importance in suppressing certain kinds of disclosure is the nexus of civil injunctions to restrain disclosures on the basis of obligations of confidence, combined with the use of contempt of court penalties for any subsequent breach of those injunctions. Whichever route is taken, the ultimate sanction for making disclosures is the threat of being fined and/or incarcerated by the state.

Moreover, the penalties imposed on those public employees or ex-employees who make unauthorised disclosures are often explicitly intended to have deterrent effects on others. Sarah Tisdall, a civil servant, was sentenced to six months imprisonment for leaking documents to the press, a sentence which the Court of Appeal held to be appropriate in reflecting an element of deterrence.[38] The punishment meted out to whistleblowers will not necessarily be proportionate to the crime they commit. This conflicts with Principle 24 of the Johannesburg Principles,[39] and contravenes the proportionality test inherent in the ECHR requirement that any restriction on free expression be "necessary in a democratic society", which applies to penalties as well as to the nature of the restrictions.[40] When breaches are punished in this way, the civil and criminal law relating to national security can be used intentionally to seek a chilling effect that cannot be construed merely as the unintended unfortunate by-product of diligently protecting the public interest in national security.

3.1 The Official Secrets Act

There has been an Official Secrets Act (OSA) in force since the first Act was passed in 1911. Offences of espionage from the original Act survive in the 1911 Act but it is the Official Secrets Act 1989 which is relevant for present purposes. The OSA contains a range of offences relating to primary disclosure – that is, disclosure by current and former members of the civil service, security services or armed forces – of various types of information. It also creates an offence relating to secondary disclosure – that is, the further dissemination, by journalists and others, of information obtained as a result of a primary disclosure. All the major offences under the OSA are punishable with a maximum term of two years imprisonment and/or an unlimited fine.[41]

[38] R v Tisdall (Sarah) (1984) 6 Cr.App.R.(S.). Court of Appeal, Criminal Division
[39] "A person, media outlet, political or other organization may not be subject to such sanctions, restraints or penalties for a security-related crime involving freedom of expression or information that are disproportionate to the seriousness of the actual crime."
[40] See Tolstoy Miloslavsky v. United Kingdom, 13 July 1995, No 323, 20 EHRR 442
[41] S. 10(1) OSA 1989

3.1.1 Disclosures by members of the Security and Intelligence Services

The United Kingdom has three intelligence and security services, known here collectively as the Security and Intelligence Services: the Secret Intelligence Service, also known as MI6; Government Communications Headquarters (GCHQ); and the Security Service, more popularly known as MI5. MI6 is responsible for security intelligence relating to defence, foreign and economic policy, while MI5 is responsible for domestic security intelligence. GCHQ is the Government's "eavesdropping" centre and monitors communications.

Primary disclosures are disclosures of security-related information by current and former members of the security and intelligence services. These public employees are subject to a much more stringent obligation of secrecy than are other civil servants or members of the armed forces. The latter are liable only where the disclosures they make are "damaging", but disclosures made by the former may be penalised without proof of damage. Anyone who works or has worked for MI5 or MI6 is guilty of a criminal offence if they disclose any information relating to security or intelligence gleaned as a result of their employment.[42] Present and ex-Security and Intelligence personnel are subject to a blanket ban on revealing any security-related information. As such, current and former members of MI5, MI6 and GCHQ may be imprisoned for making harmless revelations that have no impact on genuine national security interests.

Moreover, in these cases the OSA does not provide for a public interest defence.[43] That is, the OSA does not allow for the idea that it may be in the public interest for a disclosure to be made. Under the Act, genuine whistleblowers are not distinguished from those who make malicious or mischievous disclosures. In Germany and the Netherlands, publication of official secrets and information harmful to national security can be excused if it serves the public interest. There is no such defence for whistleblowers under UK law.

No harm test whatsoever is applied in determining whether that person's actions are deserving of criminal punishment. The ban on disclosures covers not only legitimately secret material, but also material that has entirely ceased to be confidential because it has already been brought, by whatever means, into the public domain. It also covers material that causes no damage and that which is in the public interest.[44]

The same offence is committed regardless of the truth or falsity of the disclosure, as the s. 1(1) offence does not distinguish between them.[45] This is unique to security-related information and does not, for example, apply in respect of defence-related material. In the White Paper on the OSA of 1989,[46] the Conservative Government then in power stated that this "special treatment" – proscribing disclosure by those in

---

[42] S. 1(1) OSA 1989

[43] A point noted and deplored by the Labour Party when opposing the introduction of the OSA 1989. Roy Hattersley, as Shadow Home Secretary, argued that "those who expose wrongdoing [should] be given the right to argue the defence that they did what they did in the public interest." Hansard, 21 December 1988, 477

[44] See the comments of Lord Nicholls of Birkenhead, Attorney-General v Blake and Another, 27 July 2000

[45] S. 1(2) OSA 1989

[46] Reform of Section 2 of the Official Secrets Act 1911, Cm 408

Security and Intelligence Services of all security-related information whether it is true or false – was justified on the basis that:

(1) as a matter of policy, governments do not comment on the veracity of assertions about security or intelligence; and

(2) statements by current or former members of the security and intelligence services have a "particular credibility" that allows false disclosures to cause as much damage as genuine revelations.[47]

These provisions can also be applied to civil servants in certain positions by notification procedure.

3.1.2 Disclosures by other civil servants

It is also an offence under the OSA for civil servants[48] other than those employed in the Security and Intelligence Services to disclose information relating to security or intelligence obtained as a result of their employment.[49] However, such disclosure is subject to a harm test, so that a civil servant will commit an offence only when making a "damaging disclosure". Consequently, disclosure of document X by a former member of one of the Security Services might be an offence, whilst disclosure of the same document by a former civil servant in the Home Office might not. Nevertheless, the test of "damage" is not strict and a disclosure is considered damaging if it falls within a class or description of information the disclosure of which is likely to damage the work of MI5 or MI6.[50] Thus, it is not necessary that the particular information disclosed is itself damaging.

It is also an offence to disclose information which is likely to damage defence,[51] but in this instance the notion of damage is more clearly defined to include, inter alia, material likely to damage the capability of the armed forces to carry out their tasks, lead to loss of life or injury, or endanger the interests of the United Kingdom abroad.[52] In this case, the actual information disclosed must satisfy this test. There is no repetition of the "class or description" provision that applies in relation to security and intelligence information.

An equivalent offence covers unauthorised damaging disclosures by civil servants of information relating to international relations.[53] This category is clearly defined, but excessively broad: a "damaging" disclosure for these purposes is one that is likely to endanger UK interests (or their promotion) abroad.[54] A disclosure will be deemed damaging in this way if it consists of information received in confidence from a foreign power or international non-governmental organisation.[55] It is also an offence

---

[47] Ibid., para.43
[48] Throughout this discussion, "civil servants" is used to refer to both Crown servants and government contractors
[49] S. 1(3) OSA 1989
[50] S. 1(4)(b) OSA 1989
[51] S. 2(1) OSA 1989
[52] S. 2(2)(a)-(b) OSA 1989
[53] S. 3(1) OSA 1989
[54] S. 3(2) OSA 1989
[55] S. 3(3) OSA 1989

for a civil servant to make disclosures that are likely[56] to result in the commission of an offence, facilitate an escape from legal custody or impede criminal investigations.[57] This offence also applies where the unauthorised disclosure is of information obtained by legal interceptions and actions performed by the Security Service under warrant.[58] There is no public interest defence or consideration for any of these offences.

3.1.3 Comments and conclusions

Current and ex-government employees in the Security and Intelligence Services are prohibited from revealing any security-related information, regardless of whether it is harmful and whether it serves the public interest. The only defence available to Security and Intelligence personnel is to prove that they did not know and had no reason to believe that the information they disclosed related to security and intelligence. It is difficult to imagine a defendant successfully invoking this defence.

For other public employees, the OSA does incorporate a harm test but this is often weak and easy to satisfy, requiring simply that the disclosure be likely to fall within certain circumstances. As Roy Hattersley, speaking for the Labour Party when the Official Secrets Bill was debated in 1989, noted, the "definition of harm is so wide and so weak that it is difficult to imagine any revelation, which is followed by a prosecution, not resulting in a conviction."[59]

The lack of a harm test and the failure to consider the public interest element in the disclosure makes the OSA incompatible with international standards of protection for freedom of expression. Principle 15 of the Johannesburg Principles states:

No person may be punished on national security grounds for disclosure of information if (1) the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or (2) the public interest in knowing the information outweighs the harm from disclosure.[60]

ARTICLE 19 and Liberty recognise that government employees in a position to gain access to sensitive information can rightly be placed under a duty not to divulge certain types of information harmful to national security and it is possible that even false revelations may harm national security. However, we believe those OSA provisions which fail to incorporate a harm test or public interest defence for any kind of information, and regardless of whether it is true or false, have deleterious consequences for freedom of expression and the public interest. Moreover, the active criminalisation of whistleblowers and the curtailment of expression which has a claim to some protection in its service to the public interest detracts from the credibility of the official bodies offered protection by such measures.

When the Official Secrets Act was first proposed in 1988, Roy Hattersley, on behalf of the Labour Party, then in opposition, took the view that it was "a bad Bill. Its application is likely to be worse because ? the Government will manage and

---

[56] S. 4(2)(b) OSA 1989
[57] S. 4(2)(a) OSA 1989
[58] S. 4(3) OSA 1989
[59] Hansard, 21 December 1988
[60] See Appendix 1

manipulate it."[61] Frank Dobson hoped that "[s]urely we as a Parliament have not sunk so low that we want to introduce new laws to protect official wrongdoing."[62] The current Labour government has apparently found the OSA rather more acceptable than its position in 1988?89 would have suggested.[63]

3.2 Civil remedies backed by criminal penalties

Prosecutions under the OSA have been relatively rare, not least because they tend to be embarrassing and inconvenient for the security and intelligence services. A rather more popular means of preventing both primary and secondary disclosures is the use of the civil remedy of an injunction. Rather than calling in the police to investigate what they regard as a criminal offence, the government department concerned litigates the matter directly using civil law backed by the threat of criminal penalties.

Injunctions

The injunction is one of the most powerful means open to government for controlling the flow of information. A form of prior restraint, it is also one of the most intrusive instruments available to government for denying freedom of expression. For this reason, Liberty and ARTICLE 19 believe there should be a presumption against the use of prior restraint. In their willingness to use injunctions, the UK authorities are unfettered by constitutional, statutory or judicial safeguards governing the issuing of prior restraint orders which exist in countries such as Austria, France, Sweden and the US.[64] For example, in the US, the courts have yet to uphold a single injunction against free speech on national security grounds, whereas injunctions have been sought and obtained with alarming ease and frequency in the UK. They may be sought on the basis of breach of contractual duties, of duties of confidence, fiduciary duties of confidence or copyright, or the need to prevent the commission of OSA offences.

Injunctions can be interim, permanent or for a specified period of time, and they can be obtained at a hearing where the target of the injunction is represented, or, through an ex parte application, where the target is absent.[65] Applications for injunctions to prevent disclosures of security-related information have several clear advantages for the Government over criminal prosecution. These include:

Speed. An interim injunction can be obtained via an ex parte application. The target of an injunction need not be put on notice of the application, and may not even be aware of the injunction until it is granted and served. Indeed, the government need not even

---

[61] Hansard, 21 December 1988, 478
[62] Hansard, 13 February 1989, 79
[63] See §§5-6 below
[64] Freedom of Information: An Unrecognised Right—The Right to know and the EU, An EFJ Briefing Document <www.ifj.org/regions/europe/efj/en/eusurvey.html>
[65] An ex parte application is one that proceeds in the absence of the respondent. The respondent, e.g., a newspaper planning to publish a story about the Security Service, is given no notice of the application for an injunction and is not represented at the hearing

attend a court to obtain the interim order, but can obtain "pyjama justice" at any time of the day or night by asking a judge to grant an injunction over the telephone.[66]

Onus of proof. In order to obtain an interim injunction, the government needs to establish simply that it has an arguable case in law; that damages would be an inadequate remedy; and that the balance of convenience tells in favour of granting the injunction.[67] With the traditional judicial deference to executive assessments of national security, it is not as difficult as it should be to persuade a judge that the balance of convenience favours granting the order.

Burden of proof. In making its application, the government need simply establish those matters referred to at (ii) to the civil standard of proof; namely, on the balance of probabilities, rather than beyond all reasonable doubt.

Minimal controversy. Invoking the Official Secrets Act against a person who has caught the public imagination with revelations of illegalities or incompetence in the security and intelligence community will always generate political controversy. Injunctions will typically, although not always, be politically less sensitive. Such orders carry no immediate threat of imprisonment and are obtained via a technical procedure with which few citizens are familiar.[68] In addition, since injunctions are typically obtained prior to publication and, in the absence of full information, the public would tend to assume that the injunction serves a legitimate need. Indeed, it is possible to obtain injunctions that prevent those to whom they apply from revealing even the fact that the injunction exists, let alone the precise terms of the order.[69]

Applications for permanent injunctions do not share all of these advantages. Indeed, it is not uncommon for the government to fail at the final application having succeeded at the interim stage. This was the result in the Spycatcher saga.[70] However, the interim injunction is a critical instrument. It can last for months or even years and is sufficient to suppress the intended disclosure. Eventual failure at trial to transform interim injunctions into permanent injunctions need cause no great concern to the government if the disclosures in question are by that time old news, or if a successful prosecution under the OSA has already occurred. Current procedures for injunction applications however, will be tightened up considerably under the Human Rights Act 1989 (see Chapter 10).

---

[66] Laurence Lustgarten, "Freedom of Expression, Dissent, and National Security in the United Kingdom," in Sandra Coliver et al, Secrecy and Liberty: National Security, Freedom of Expression and Access to Information, Kluwer Law, 1999, p.467

[67] American Cyanamid Co. v Ethicon Ltd [1975] AC 396. House of Lords

[68] Laurence Lustgarten, "Freedom of Expression, Dissent, and National Security in the United Kingdom," in Sandra Coliver et al, Secrecy and Liberty: National Security, Freedom of Expression and Access to Information, Kluwer Law, 1999, p.469

[69] The injunction granted against "Martin Ingrams" and The Sunday Times in November 1999 "initially barred [the paper] from revealing that it had been gagged or repeating what had already been published," although this term of the order was relaxed on appeal. See Liam Clarke, "Gagging order protects army's dirty tricks unit," The Sunday Times, 28 November 1999

[70] Compare Attorney-General v Guardian Newspapers Ltd (No.1) [1987] 1 WLR 1248 House of Lords (interim injunction upheld despite publication of the book in America) with Attorney-General v Guardian Newspapers Ltd (No.2) [1988] 3 WLR 776 House of Lords (application for permanent injunctions refused because widespread publication had destroyed the confidential nature of the information disclosed in the book)

Injunctions are a civil remedy. However, they are backed up by the threat of criminal proceedings for contempt of court in the event that the terms of the injunction are breached. Prosecutions under the OSA are also criminal, so the effective outcome is the same – to criminalise the dissemination of information, regardless of whether or not this is in the overall public interest. Indeed, it could be argued that injunctions pose the greater threat to freedom of expression since trials for criminal contempt are not conducted in the presence of a jury. The fact that a judge alone presides at such hearings is of particular concern given the tendency of the judiciary to defer to the executive in matters of national security, as outlined previously in this report.

The law of confidence

The usual grounds for injunction applications against current or ex-public employees is breach of laws, conventions and regulations regarding confidence. Members of the security and intelligence services are deemed to owe the state a lifelong duty of confidence.[71] Former spies remain under an obligation not to disclose any security-related information until the day they die. There are several sources of this obligation of confidence. In David Shayler?s case, the Attorney-General based his claim for an injunction on:

(i) an express contractual term requiring lifelong non-disclosure;

(ii) an implied contractual term of good faith which would be breached by any disclosure;

(iii) a fiduciary duty requiring lifelong non-disclosure;

(iv) a fiduciary duty of good faith which would be breached by any disclosure; and

(v) infringement of Crown copyright in documents containing confidential information.

These alleged terms and duties purport to create an enduring obligation not to disclose any security-related material whatsoever and are reinforced by the blanket terms of s. 1(1) OSA 1989, relating to primary disclosure by present and former members of the security and intelligence services (see section 3.1).

The law of confidence does require that the government, in seeking to impose an injunction, establish inter alia that there is a legitimate interest to be protected. Moreover, where an injunction is sought on these grounds, the public interest in knowing the information must be considered. However, pleading “national security” as that legitimate interest in this sphere attracts similar deference by the courts to that observed during judicial review processes. Once that legitimate interest has been identified, it is relatively easy to show that the balance of convenience favours an injunction, since at present the law will find defendants in breach of their obligations of confidence unless those defendants can show that disclosure served a greater public interest. Where the application is made ex parte, the defendant can have no opportunity even to attempt to make such an argument before the remedy is granted.

[71] Attorney-General v Guardian Newspapers Ltd (No.2) [1988] 3 WLR 776. House of Lords

In addition to injunctions, a number of remedies may be applied for breach of confidence and other civil obligations relating to the disclosure of information. These include:

- Delivery-up. An order may be sought for the delivery-up of documents on the basis that the Crown holds copyright in those documents.

- Damages. The government can argue for an award of damages to compensate it for loss incurred as a result of breach of contract, infringement of copyright and/or breach of fiduciary duties of confidence.

- Account of profits. An order requiring the defendant to account to the Crown for all profits made as a result of disclosures may be available on the basis of breach of fiduciary duty and breach of copyright. Moreover, the House of Lords has recently decided that account of profits may be available for breach of contract where that breach consists in a disclosure by a former member of the security and intelligence services that contravenes s. 1(1) OSA 1989.[72]

3.3 Recent prosecutions of former Security and Intelligence officers

The OSA 1989 has been deployed frequently in the last few years to counteract disclosures of security-related material.[73]

David Shayler

Perhaps the most well-known recent case under the Official Secrets Act is that of David Shayler. An ex-MI5 officer who left the Intelligence Service in 1997, he is currently facing three charges of breach of the OSA. In August 1997, the Mail on Sunday was supplied with security-related information, including the allegation that the government kept secret files on certain Labour politicians. In July 1998, after he had left the UK for France, David Shayler allegedly accused MI5 of failing to react on prior knowledge of a terrorist attack on the Israeli Embassy, and alleged that MI6 officers had plotted to assassinate the Libyan leader, Colonel Gaddafi. A month later he was arrested in France and held without charge for four months while the UK Government attempted without success to extradite him. In July 2000, in an article in Punch magazine, he claimed that MI5, GCHQ and the Metropolitan Police could have prevented IRA's bombing of Bishopsgate, in London, but that they failed to do so. In addition to placing an injunction on Shayler in August 1997, which forbade him from revealing any further information unless formally authorised, the Government issued a statement of claim against him on 22 December 1999 for breaching copyright laws on files held by MI5 and MI6, and breaches of confidence and contract.

The perception of the need for a comprehensive gag on serving and former spies is not universally shared among members of the judiciary. Judge LJ stated that David Shayler's allegation of MI6 participation in a plot to assassinate Colonel Gaddafi "is either true or it is false, and unless there are compelling reasons of national security,

---

[72] Attorney-General v Blake and Another, House of Lords 27 July 2000

[73] The last OSA prosecution for a security-related disclosure occurred in October 1998. See Richard Norton-Taylor, "'Blunder' over naval vetting," The Guardian, 19 February 2000

the public is entitled to know the facts."[74] Despite this entitlement, the combined effect of s. 1(1) and s. 1(2) OSA 1989 is to expose Shayler to prosecution for making those disclosures. Given the extraordinary scope of the OSA offences – and the s. 1(1) offence in particular – it is perhaps unsurprising that the French courts refused the UK's request for extradition of Shayler in 1998 on the basis that the charges were "political" in nature.[75] David Shayler returned to the UK voluntarily in August 2000 to face charges of breach of the OSA, and intends to invoke the Human Rights Act in his defence.

Richard Tomlinson

Richard Tomlinson is an ex-MI6 employee. In 1995 he was denied an industrial tribunal at which to contest his dismissal on grounds that it would require disclosure of information harmful to national security. He was sentenced to one year's imprisonment in 1997 for offences under the OSA for having sent an Australian publisher a synopsis of a planned memoir-cum-exposé of his work. Released on parole in April 1998 after nine months in prison, he was barred from talking to journalists and his passport was confiscated. However, Tomlinson left Britain and went to France where he made public allegations that MI6 had been involved in wrongdoing, one such claim being that there had been an MI6 plot to assassinate Slobodan Milosevic, then President of Yugoslavia.[76]

Tomlinson was re-arrested under an international warrant on 31 July 1998 in France, by officers from Scotland Yard and members of the Direction de la Surveillance du Territoire (DST), the French equivalent of MI5. The warrant was issued on the basis of suspicions that Tomlinson was intending to make damaging disclosures regarding the security and intelligence services. However, the DST personnel quickly determined that there was insufficient evidence to justify an extradition and, as in the case of David Shayler, the UK Government's attempt to extradite him failed and Tomlinson was released after some 30 hours' questioning.[77] He then travelled to New Zealand in August 1998, where he was greeted with an injunction obtained by the UK Government which prevented him from making any security-related disclosures and complemented the injunction already in place in the UK.[78] After the names of spies were placed on the Internet on 12 May 1999 government suspicion fell on Tomlinson despite his denial, and he was expelled from Switzerland where he was then living. The Government continues to believe that he intends to publish damaging revelations and in May 2000, Italian police accompanied by British Special Branch officers raided his apartment in Italy and took away personal papers and computer equipment.[79]

---

[74] R v Central Criminal Court, ex parte The Guardian, The Observer & Martin Bright, Divisional Court of Queen's Bench Division 21 July 2000, draft judgment, p.2

[75] "Officials study Shayler ruling," BBC News, 19 November 1998, <<news.bbc.co.uk/hi/english/uk/newsid_216000/216795.stm>>

[76] "The spy who was snubbed" BBC News 13 May 1999 <<news6.thdo.bbc.co.uk/hi/english/uk/newsid_342000/342853.stm>>

[77] David Leppard and Nicholas Rutherford, "The spies dragged in from the cold," The Sunday Times, 9 August 1998

[78] Michael Evans, "Cook gags former MI6 spy in New Zealand," The Times, 6 August 1998

[79] Philip Wilan "Renegade spy to give himself up in return for tribunal hearing", The Guardian, 3 June 2000

Nigel Wylde

Shayler and Tomlinson may be the most widely-known individuals pursued via the OSA in recent years, but they are not the only ones. Nigel Wylde, a former army colonel, has been arrested and charged with making damaging defence-related disclosures under s. 2 of the OSA. This prosecution has been brought against Wylde as the alleged source of information published in The Irish War by Tony Geraghty, a book which includes details of the extent to which the population in Northern Ireland is kept under computerised surveillance by the state.[80] Wylde was identified through a search of Geraghty's house under the OSA. No attempt was made to prevent publication of Geraghty's book. Indeed, the Ministry of Defence has conceded that the book was "embarrassing rather than damaging."[81] In October 2000, however, the MoD lawyers were reported to be seeking to try Wylde in secret, since the MoD is now claiming that the information in the book was damaging.[82] One obvious reason for these charges is the hope of exercising a deterrent effect on any further disclosures of this kind.

"Martin Ingrams"

Also facing prosecution under s.1 of the OSA is the pseudonymous "Martin Ingrams", former member of the Force Research Unit (FRU), a now disbanded "clandestine cell" within army intelligence which handled informants within the IRA and loyalist paramilitary groups.[83] "Ingrams" has made various disclosures to Liam Clarke of The Sunday Times regarding the activities of the FRU and other security forces operating in Northern Ireland. He has alleged that the security forces elected not to confiscate or disable terrorist weapons which were subsequently used in sectarian killings in the interests of protecting their informers within the paramilitary groups.[84] Additionally, "Ingrams" has claimed that listening devices used by the security forces to gather information facilitated two SAS ambushes that resulted in the deaths of eleven IRA members.[85]

The most notorious of "Ingrams's" disclosures concerns attempts by the FRU to disrupt an inquiry conducted by John Stevens (now Commissioner of the Metropolitan Police) into alleged links between the police and security forces and loyalist murders. According to "Ingrams", these efforts reached their peak with an "illegal burgle-and-burn assault"[86] on the offices used by the Stevens Inquiry team. The fire was intended to sabotage the inquiry in order to prevent or at least delay the arrest for murder of a FRU informer named Brian Nelson. The attempt failed because Stevens had fortuitously kept back-up copies of all files elsewhere. Nelson was convicted.

---

[80] "A pointless prosecution," The Guardian, 26 February 2000
[81] Richard Norton-Taylor, "Secrets charges against Ulster spy author dropped," The Guardian, 23 December 1999
[82] Richard Norton-Taylor, "MoD wants former officer tried secretly over book revelations", The Guardian, 23 October 2000
[83] Richard Norton-Taylor, "Secrets and Spies," The Guardian, 18 May 2000
[84] Liam Clarke, "Agents ?stole papers? to nail whistleblower," The Sunday Times, 2 April 2000
[85] Liam Clarke, "Listening devices take the place of agents," The Sunday Times, 21 November 1999
[86] Liam Clarke, "Secret army unit burnt police files," The Sunday Times, 21 November 1999

Certain of “Ingrams’s” claims have been described as "absolutely on the knuckle" by one RUC officer[87] and his allegations regarding interference with the Stevens Inquiry are being taken seriously by police.[88] The issue of concern here is not the legality or appropriateness of FRU actions but rather the clear public interest in knowing that such decisions were made and in having access to information regarding the conduct of security operations in those circumstances. Provided that no current genuine national security interests are threatened and no lives put at risk, it is important that such matters be brought into the public domain.

The OSA does not allow “Ingrams” to argue that the public interest justified his disclosures. The official response to those disclosures has not been to investigate his allegations of illegal and dangerous acts by the FRU, but rather to make efforts to identify and prosecute him for breach of the OSA. The hunt for him led to at least one other arrest under the OSA, that of a former soldier accused of being “Ingrams”. On 1 February 2000, prior to his arrest, the individual’s house was burgled. Amongst the items stolen was the draft of a memoir.[89] Extraordinarily, this manuscript "turned up a few days later in the hands of the prosecution at a court hearing" for an injunction preventing publication of the work[90] and was used to confront the alleged “Ingrams” in questioning.[91] The MOD claimed that these papers had been received in a mysterious letter drop. If one has doubts about the justifiability of the OSA offences themselves, this series of events gives independent cause for concern regarding how alleged breaches of the OSA are investigated.

3.4 Concluding observations

The Government’s pursuit of the above cases highlights three tendencies, active criminalisation of whistleblowers; the use of far-reaching injunctions; and increasing inventiveness in the grounds on which injunctions are sought.

There can be no doubt that there is a powerful public interest in at least some of the disclosures made by Shayler, Tomlinson, Wylde and “Ingrams”. Yet the OSA makes criminals of those “insiders?” who would expose illegal and/or dangerous behaviour by the Security and Intelligence Services. There are at present few, if any, means by which wrongdoing within these services can be exposed, and the overall public interest properly assessed. In particular, there is no independent means for balancing the public interest in disclosure against any genuine national security considerations.

The experiences of Shayler, Tomlinson, Wylde and “Ingrams” highlight the extensive use of the generally preferred means of gagging state servants, namely the civil injunction. Experience suggests that when the Government claims “national security” as the legitimate interest to be protected in applications for far-reaching injunctions, the desired interim order will be obtained from the courts without great difficulty. The Government has no hesitation in trying to extend the scope of injunctions as far as possible. For example, in respect of “Martin Ingrams” and The Sunday Times, the government requested and initially received an order that prevented repetition of

[87] Henry McDonald, "Police in hunt for British agent," The Observer (Irish edition), 21 May 2000
[88] Liam Clarke, "Met chief blames arson on army," The Sunday Times, 19 March 2000
[89] Liam Clarke, "Agents ‘stole papers’ to nail whistleblower," The Sunday Times, 2 April 2000
[90] Richard Norton-Taylor, "Secrets and Spies," The Guardian, 18 May 2000
[91] Liam Clarke, "Agents ‘stole papers’ to nail whistleblower," The Sunday Times, 2 April 2000

previously published allegations and even mention of the fact that the injunction existed.[92] These conditions were removed on appeal.

In an apparent attempt to counter adverse publicity, the UK Government has denied that a wide interim injunction relating to David Shayler, in place since September 1997, is a “blanket” injunction, since it allows for the repetition of information already in the public domain and for new disclosures "if formal authority is obtained beforehand."[93] In seeking this injunction, the government relied upon a wide range of claims, including the triumvirate of claims described above, as well as a claim for breach of Crown copyright.[94]

[92] Richard Norton-Taylor, "Softly, softly," The Guardian, 10 April 2000
[93] Lord Williams of Mostyn, letter to The Guardian, 6 August 1998
[94] This can also constitute a criminal offence. See s. 107 Copyright Designs and Patents Act 1988

4 Restricting Secondary Disclosure - Gagging the Media and others

Democracy requires citizens to be informed so that they can meaningfully exercise their right to participate in the democratic process. The media play an essential role in facilitating the process of providing information to citizens. This is particularly important in regard to information about official wrongdoing. Experience shows that when wrongdoing does take place, investigative journalists are among those best placed to expose it. Indeed, because of the great public interest in the conduct of government, including corruption and other kinds of misuse of public office, the European Court of Human Rights has frequently noted the important 'watchdog' role of the media.

However, as Chapters 4 and 5 show, formidable barriers are placed in the way of investigative journalists in the form of laws preventing secondary disclosure of information relating to national security, and the relative ease with which the Government is able to pry confidential sources and information from journalists. With regard to security information, the law in relation to the media, allows the government to employ a wide range of criminal and civil law to prevent disclosures. In so far as publication is frequently the primary means by which the public are alerted to such disclosures, mechanisms invoked against the press are the most effective way for the government to prevent information from reaching the public.

4.1 Secondary disclosure under s. 5 OSA

The main legal mechanism for preventing secondary disclosure is contained in s. 5 of the OSA, which makes it a criminal offence for anyone to disseminate information deemed to be damaging to national security. The principal target of this provision has always been the media. Although there is a harm test, there is no public interest defence.

Under s. 5, anyone will commit an offence if:

(i) they receive information from an "insider" by way of a primary disclosure;[95]

(ii) they make a secondary disclosure without obtaining lawful authority knowing (or having reason to believe) that the primary disclosure was unlawful under the OSA;[96]

(iii) they know or have reason to believe that their secondary disclosure would be damaging;[97] and

(iv) their secondary disclosure is damaging.[98]

It does not matter whether the target of this provision – normally a journalist or media outlet – received the information directly or indirectly from the original (insider)

[95] S. 5(1)(a)(i) OSA 1989
[96] S. 5(2) OSA 1989
[97] S. 5(3)(b) OSA 1989
[98] S. 5(3)(a) OSA 1989

source. On the other hand, the journalist must have at least reasonable cause to believe both that the disclosure was unlawful and that it would be damaging to national security. This may be harder for the prosecution to establish in the case of "outsiders" than for civil servants and spies, since the latter may be generally assumed to be more familiar with these matters. Moreover, in respect of this offence, it is for the prosecution to prove beyond reasonable doubt the presence of all elements of the offence. Indeed, having the requisite knowledge is a key element of the s. 5 offence. While it is more difficult to prosecute a journalist under the OSA than a civil servant or member of the security and intelligence services, the lack of any public interest defence remains a notable and disturbing feature of the legislation.

4.2 The Defence Advisory notice system (DA-Notice system)

In addition to the media's important role as a watchdog of government on behalf of society, they also have a responsibility, as do government employees and the general public, to exercise their right to freedom of expression so that genuine national security interests are protected. The DA-Notice system, formerly the D-Notice system, was set up to prevent disclosures by journalists unsure or unaware of whether a particular disclosure would be regarded as damaging to national security. However, Liberty and ARTICLE 19 are of the view that this system represents a seriously flawed attempt to negotiate the boundaries between press publication of security information and freedom of expression through an "informal?" system.

The Defence, Press and Broadcasting Advisory Committee was conceived as a voluntary arrangement between government and the press with the aim of preventing inadvertent breaches of s. 5 OSA 1989.[99] Chaired by the Permanent Under-Secretary of State for Defence, it has seventeen members, thirteen of which are nominated by media organisations. The Committee, established in 1912, issues general guidance notices and specific "Private and Confidential" notices, on categories of information where secrecy id deemed to be essential to protect national security. Editors or journalists can, if they wish, consult the Secretary of the Committee, currently Rear-Admiral Nick Wilkinson, to find out in advance whether any details contained in a planned story fall within the scope of the five standing DA-Notices which cover different areas of possible threat to national security. The Secretary's role is officially described as that of a confidential mediator between the journalist wishing to publish and the government department or security service concerned to protect national security.[100] Under the Committee's rules, any officials whom the Secretary consults about a particular story must be able to convince the Secretary of the need for secrecy and cannot initiate police action or legal proceedings unless they have the requisite information from another source.[101]

The DA-Notice system is unique – no other country in the world maintains such an arrangement.[102] Some editors are convinced that the system is outdated, a relic of the Cold War,[103] although others concede the value of an "advisory pipeline" of this

---

[99] See §4.2 and §6 below
[100] <<www.dnotice.org.uk/faqs.htm>>
[101] Ibid
[102] Ibid
[103] "What is remarkable about [DA-Notices] is that editors still obey them." Roy Greenslade, quoted in The Independent, 18 May 1999

nature.[104] Regardless of ones' position on the value of the Committee's advice, the DA-Notice system suffers from at least two key flaws. First, existing as it does under the shadow of the draconian provisions of s. 5 of the OSA, it is hardly voluntary in any true sense of that word. Absent the threat of OSA prosecutions and other forms of legal harassment, it may be assumed that few journalists would bother with the DA-Notice system.

Second, "compliance [with the DA-Notice system] does not relieve the editor of responsibilities under the Official Secrets Act."[105] Thus, the fact that the Secretary has raised no objection to a planned story does not necessarily mean that the applicant editor or journalist is immune from prosecution in respect of any disclosures they then go on to publish. Given this, the claim by the Secretary that the DA-Notice system operates on a more stringent and narrower understanding of "national security" than the OSA and other statutes[106] is of scant comfort. The current Secretary maintains that "negotiation by me between the media and the officials must be preferable to litigation, especially as litigation tends to be slow and expensive and to end in blanket suppression of a story or source, rather than removal of just a few details."[107] Many in the media world, on the other hand, feel that one does not necessarily preclude the other.

Of at least equal concern is the growing perception amongst journalists that the DA-Notice system is in fact being used to facilitate censorship of the press by the government, despite the Secretary's insistence that it is "independent and media-dominated."[108] Journalists have expressed the fear that seeking "confidential" mediation will merely invite early receipt of an injunction and/or investigation for breach of s. 5 OSA, and this is not helped by the tradition of appointing an ex-Armed Services person to the post of Secretary. The Secretary offers guidance in consultation with members of the affected services, and this necessarily gives them advance warning that a story is about to emerge. Even if the Secretary does not disclose the identity of the party, it is not difficult for professional intelligence officers to discover the relevant information in short order. The experience of Tony Geraghty has greatly reinforced this suspicion (see box below) although the Secretary of the DA-Notice Committee "denied any collusion between himself and the MoD police".[109]

Tony Geraghty

Tony Geraghty was accused of disclosing information regarding the extensive use of computerised surveillance by intelligence agencies in Northern Ireland in his book, The Irish War. Prior to publication of his book, Rear Admiral David Pulvertaft contacted Geraghty's publishers, inviting the author to submit the manuscript for evaluation. Geraghty declined, believing that the only reason for the request was to facilitate the identification of his sources within the SAS.[110] Geraghty has reported that the Secretary responded to his refusal by expressing his hope that Geraghty

---

[104] Cal McCrystal, "Secret stories," The Guardian, 5 July 1999
[105] "General Introduction to DA-Notices", <<www.dnotice.org.uk/notices.htm>>.
[106] This claim was made by Rear Admiral Nick Wilkinson in the course of a speech to the Society of Editors on 3 May 2000, See "Media Articles and Speeches," <<www.dnotice.org.uk/articles.htm>>
[107] "Media Articles and Speeches," <<www.dnotice.org.uk/articles.htm>>
[108] Rear Admiral Nick Wilkinson, "Open Secrets," letter to The Observer, 30 July 2000
[109] John Davison, The Independent, 18 May 1999
[110] Stephen Glover, "Where's freedom of information if this journalist is charged next Thursday?" The Spectator, 6 March 1999

"would not come to regret" his non-co-operation.[111] No attempt was made to prevent publication of the book; but Geraghty's house was raided by Ministry of Defence police on 3 December 1998 and the author was subsequently charged with the secondary disclosure offence under s. 5 OSA 1989.[112]

4.3 Recent prosecutions brought under s. 5 OSA

Tony Geraghty

As outlined above, former Sunday Times defence correspondent Tony Geraghty was arrested some three months after publication of his book, The Irish War. No injunction was sought at the time of publication, perhaps because, as the Ministry of Defence has subsequently conceded, its revelations regarding the extensive surveillance conducted on the population of Northern Ireland were "embarrassing rather than damaging."[113] Nevertheless, the publishers came under pressure from Ministry of Defence police to refrain from issuing a paperback version of the work.[114] Geraghty was arrested after a dawn raid of his home on 3 December 1998 for breach of s. 5 OSA 1989.[115] The charge was dropped in December 1999 on the advice of the Attorney General. Significantly, this change of heart occurred shortly before the case would have reached committal proceedings, that is, the first point at which the prosecution case would have been subjected to judicial examination. Geraghty is not alone in being "surprised that they [the military police] believe that they have lawful jurisdiction over a civilian author owing no legal duty to the MoD."[116] The charges against Nigel Wylde, Geraghty's alleged source, are still being pursued.

Liam Clarke

In 1999, the Northern Ireland Editor of The Sunday Times was threatened with prosecution for breach of s. 5 of the OSA.[117] Clarke published a series of articles detailing disclosures made by agents, including "Martin Ingrams" (see 3.3), of the activities of the undercover Force Research Unit (FRU) in Northern Ireland. The articles contained serious allegations of wrongdoing by the FRU, including claims that they committed arson to destroy evidence in an official investigation and spied on and tapped the phones of opposition Members of Parliament. Following a complaint by the UK Ministry of Defence, Clarke was detained by the Metropolitan Police for questioning regarding breach of s 5 of the OSA. It remains unclear whether he will be charged.

---

[111] Cal MacCrystal, "Spying secrets spark 'abuse' of the D-notice", Evening Standard, 12 March 1999
[112] Stephen Glover, "Where's freedom of information if this journalist is charged next Thursday?" The Spectator, 6 March 1999
[113] Richard Norton-Taylor, "Secrets charges against Ulster spy author dropped," The Guardian, 23 December 1999
[114] Richard Palmer, "Anger at book ban on Ulster spy secrets," The Express, 26 July 1999
[115] Richard Norton-Taylor, "Secrets charges against Ulster spy author dropped," The Guardian, 23 December 1999
[116] Tony Geraghty, "I am censored too," letter to The Sunday Telegraph, 7 March 1999
[117] Letter from Detective Inspector Alan Learner to Liam Clarke, 5 May 2000

Julie-Ann Davies

Perhaps the most astonishing case of the use of s. 5 OSA is that of Julie-Ann Davies, a mature student and volunteer researcher for the satirical programme, the Mark Thomas Comedy Product. She was arrested and questioned for possible breach of s. 5 OSA on the basis that she had been in communication with David Shayler. Yet the OSA only prohibits disclosures and it is unclear which disclosures she herself was alleged to have made. Her university – "an institution committed to freedom of expression" – was equally perturbed by the development. The Vice Chancellor stated that Kingston University "would be particularly concerned if it turned out that a discredited piece of legislation … was being used to suppress journalistic investigation and the public's right to know about alleged abuse by the security services."[118] Although it has since been decided that Julie-Ann Davies should not be prosecuted, her arrest gives cause for concern, since it shows a determination to extend the impact of chilling effects beyond prospective whistleblowers and the media, to encompass anyone inclined to assist – or even to correspond with – a whistleblower.

4.4 Use of injunctions to prevent publication

As well as being used to gag whistleblowers, injunctions are also brought heavily to bear on press attempts to publish "damaging information." Indeed, the government's preferred means of gagging the press still seems to be prior restraint via an injunction, notwithstanding the recent increase in criminal proceedings under s. 5 OSA. Once an injunction is granted, it can be served not only on the defendant, but also on any media outlet likely to disclose the information in question. Injunctions can also be served directly on journalists and their employers.

Significantly for the media, injunctions may be imposed for breach of confidence even in the absence of any contractual relationship. A newspaper or journalist that receives security-related information as the result of a primary disclosure may be held to owe a duty of confidence to the state in equity where they know that the primary disclosure by the whistleblower occurred in breach of confidence.[119] As such, the government can seek an injunction against the media directly, even if not (yet) able to identify the primary source of the information concerned and independently of any legal action against the source.

Injunctions abound at present in relation to the publication of security-related information by "Martin Ingrams", Shayler and Tomlinson.

The Sunday Times received an injunction in respect of revelations by "Martin Ingrams" relating to the Force Research Unit. Newspapers have also been banned from publishing any disclosure he makes about the 1973 "Bloody Sunday" killings of civilians by UK security forces in Northern Ireland. Initially, the injunction on information about the FRU not only covered facts already published, but also prevented any disclosure of the existence of the injunction. These conditions were

---

[118] Vice Chancellor Peter Scott, quoted in "Student arrested over Shayler link," The Guardian, 7 March 2000

[119] Attorney-General v Guardian Newspapers Ltd (No.2) [1988] 3 WLR 776, House of Lords

relaxed on appeal, but the precise terms of the injunction still may not be disclosed.[120] The press has thus been prevented from disclosing any further information relating to allegations of illegal and dangerous activities, including interference with an independent police inquiry.[121] It appears that the interests of national security demand that a willingness to endanger life and impede the course of justice by those in the employ of the army's intelligence units be kept secret. The Ministry of Defence apparently "cannot identify any 'public interest which demands publication of such material'".[122]

Injunctions also exist to prevent any publication of further allegations from Shayler. On 6 October 2000 James Steen, editor of Punch magazine, was found guilty of contempt of court in relation to publication of an article written by David Shayler, even though the judge found no evidence to believe that it had harmed national security.[123] The article was found to be in breach of the 1997 injunction "which bans publication of any information David Shayler acquired by virtue of employment for the security service",[124] although government lawyers admitted that it had been broken many times before. In accordance with the magazine's practice, Punch submitted Shayler's article to the Government Law Officers before publication for confirmation that it would not infringe the injunction. When the Treasury Solicitor was unable to deliver a final verdict on the article in good time, Steen decided to publish an abridged version of the original. He is currently appealing the guilty verdict.

4.5 Conclusion

Despite the unacceptability of attempting to chill free expression by criminalising journalists carrying out their job of investigating alleged government wrongdoings, the Labour Government currently in power has displayed an increased willingness to deploy s. 5 OSA, and has sought to exploit additional remedies against those who have made secondary disclosures in matters touching on national security. ARTICLE 19 and Liberty believe that the UK Government makes excessive use of both civil and criminal procedures to prevent embarrassing information from reaching the public at large and that the penalties it seeks to impose have generally been disproportionate to actual damage caused when balanced against the public interest in knowing the information.

---

[120] Liam Clarke, "Gagging order protects army's dirty tricks unit," The Sunday Times, 28 November 1999

[121] See 4.4 below for further detail on "Ingrams's" disclosures

[122] Liam Clarke, "Undercover arsonists promoted by army," The Sunday Times, 16 April 2000

[123] Richard Norton Tayler, "Punch ruled guilty of contempt of court" The Guardian, 7 October 2000

[124] Spokesman for the Attorney-General's office, quoted in Paul Lashmar, "Editor of Punch to face court for Shayler contempt," The Independent, 28 July 2000

5 Protection of sources

Journalists' ability to expose wrongdoing, and hence to exercise their proper function in a democracy, is often heavily dependent on their ability to receive and hold information in confidence, and their capacity to make credible promises of confidence to their sources of information. Further, in many cases, protection of confidential sources is essential not only to maintain the free flow of information to journalists, and from them to the public, but also for the personal security of journalists.

Under the current legal regime in the UK, a public interest defence holds no weight and insiders risk criminal prosecution if they decide to blow the whistle on illegality and incompetence in matters touching on national security, regardless of how peripheral or important they may be. Their willingness to do so thus often depends directly on assurances that their identities will be concealed. If journalists can be compelled to divulge their sources – or to grant access to documents that could enable the source to be traced and identified – their promises of confidence will ring hollow.

Across the world, journalists have too frequently and too readily been required to divulge their sources, and there is a widely felt consensus that the UK courts have systematically failed to accord due weight to the importance of permitting journalists to keep their sources confidential. It may be true that "[a]ny rule of professional conduct enjoining a journalist to protect his confidential sources is subject to whatever exception is necessary to enable the journalist to obey the orders of a court of competent jurisdiction."[125] However, this can be regarded as an acceptable statement of principle only if the court of competent jurisdiction is required to recognise and give special weight to the public interest in journalists' ability and interest in keeping their sources confidential.

5.1 International standards on protection of journalists' sources

The UN, OSCE and OAS rapporteurs on freedom of expression asserted in February 2000 that: "Journalists should never be required to reveal their sources unless this is necessary for a criminal investigation or the defence of a person accused of a criminal offence and they are ordered to do so by a court, after a full opportunity to present their case."[126]

The European Court of Human Rights has emphasised the fact that orders for source disclosure have the potential to produce a substantial chilling effect, significantly impairing the capacity of the press to act as public watchdog. One important ruling in the landmark judgment of Goodwin v UK,[127] was that, "[l]imitations on the confidentiality of journalistic sources called for the most careful scrutiny by the

[125] X Ltd v Morgan Grampian (Publishers) Ltd and others [1991] 1 AC 1, House of Lords per Lord Bridge
[126] Statement regarding key issues and challenges to freedom of expression, agreed by: Santiago Canton, OAS Special Rapporteur on Freedom of Expression. Freimut Duve, OSCE Representative on Freedom of the Media and Abid Hussain, UN Special Rapporteur on Freedom of Opinion and Expression, ARTICLE 19, February 2000
[127] Goodwin v UK, 27 March 1996, 22 EHRR 123

Court."[128] This requires courts to take their own watchdog responsibilities seriously and subject any applications for source disclosure to substantive analysis. As the European Court put it:

"Protection of journalistic sources is one of the basic conditions for press freedom … Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result, the vital public watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest."[129]

Most established democracies – including, for example, Austria, Denmark, Finland, France, Germany, Italy and Sweden – provide explicit protection for journalists' confidentiality of sources. It is the view of Liberty and ARTICLE 19 that journalists should not be compelled to disclose their sources, except under "exceptional circumstances", where "vital interests" are at stake.[130]

5.2 Legal mechanisms for compelling source disclosure in the UK

There are both criminal and civil mechanisms available to the government to use in pursuit of journalists either for direct disclosure of their sources, or else for access to notes and papers which may enable the informant to be identified and traced.

It has been argued that s.10 Contempt of Court Act 1981 provides some degree of protection to journalists by holding that:

No court may require a person to disclose … the source of information contained in a publication for which he is responsible, unless it be established to the satisfaction of the court that disclosure is necessary in the interests of justice or national security or for the prevention of disorder or crime

This section has been described as requiring the judge to engage in a balancing exercise, weighing the importance of non-disclosure and the need for disclosure in the interests of, for example, national security.[131] However it fails to give due weight to the presumption in favour of non-disclosure. S. 10 states that the court must be persuaded that an order for source disclosure is necessary in the interests of, for example, national security.

It would appear that the application of s. 10 by judicial authorities within the UK falls short of the standard set out in Article 10 of the European Convention. In 1996 the

---

[128] Michael Allen & Brian Thompson, Cases & Materials on Constitutional & Administrative Law, 5th edition, 1998: Blackstone Press, p.565
[129] Goodwin v United Kingdom, 27 March 1996, 22 EHRR 123. European Court of Human Rights
[130] Protection of Journalists' Sources: Comparative Law and Jurisprudence, written comments submitted to the ECHR in the case of Goodwin v UK by ARTICLE 19 and Interights (April 1995)
[131] X Ltd v Morgan Grampian (Publishers) Ltd and Others [1991] 1 AC 1, House of Lords per Lord Bridge

European Court of Human Rights ruled in the case of Goodwin v United Kingdom that the application of s. 10 of the Contempt of Court Act 1981 by the UK House of Lords in fining a journalist for refusing to disclose his source violated Article 10 of the ECHR. The European Court disagreed with the House of Lords regarding the application of the necessity test, finding that on balance the interest of a democratic society in a free press outweighed any countervailing interests.[132] Significantly, in a more recent case, striking for its similarity to the facts of Goodwin, UK courts again ordered source disclosure.[133]

Orders for disclosure of sources often take the form of the statutory production orders. These allow the police to access journalistic material that is likely to assist in a criminal investigation, including investigations into alleged breaches of the Official Secrets Act.[134] There is also common-law power to order similar disclosure to enable "wrongdoers" to be prosecuted, including those allegedly responsible for a breach of confidence.[135]

Criminal procedures

a) The Police and Criminal Evidence Act 1984 (PACE)

S. 9 of the Police and Criminal Evidence Act 1984 allows for production orders to be made by a judge if persuaded by the police that certain "access conditions" contained in schedule 1 are satisfied. The orders are designed to allow the police to pierce the veil of journalists' professional confidence in the event that this will assist with a criminal investigation. The investigation in question could, of course, concern an alleged breach of the OSA, but only "serious arrestable offences" are covered by the provisions of s. 9 and sch. 1. Neither s. 9 nor sch. 1 of PACE contain statutory requirements to weigh press freedom against the interests of facilitating a terrorist investigation.

b) Prevention of Terrorism Acts (PTA)

Similar powers to those described above (based on less stringent access conditions) have been conferred on judges by the Prevention of Terrorism (Temporary Provisions) Acts. Although these powers apply solely in respect of "terrorist" investigations, they have been placed on a permanent footing in the Terrorism Act 2000, in which the definition of terrorism has been considerably widened.

c) S. 8(4) of the Official Secrets Act 1989

The OSA contains a mechanism to facilitate access to journalists' papers. S. 8(4) OSA 1989 makes it an offence for a journalist to fail to comply with an "official direction" for the return or disposal of information subject to s. 5 OSA which is in their possession or control. This may be punished with three months' imprisonment and/or an unlimited fine.[136]

---

[132] Goodwin v UK , 27 March 1996, 22 EHRR 123
[133] Camelot Group plc v Centaur Communications Ltd [1998] 2 WLR 379, Court of Appeal
[134] e.g., s. 9 Police and Criminal Evidence Act 1984
[135] Norwich Pharmacal v Customs & Excise Commissioners [1974] AC 133, House of Lords, as subsequently fettered by s. 10 Contempt of Court Act 1981
[136] S. 10(2) OSA 1989

d) The Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act, passed in July 2000, authorises the executive to undertake interception of electronic communication on the vague and undefined grounds of national security and economic well-being, and to compel access to decryption keys. This legislation legitimises official surveillance of e-mail correspondence and Internet use by private individuals. Had the RIP Act been in place at the time, there would have been no need for the Government to take out a production order against The Guardian to compel surrender of David Shayler's email (see section 5.3 below). The surveillance can be carried out covertly on the orders of the executive without prior judicial authorisation.

Civil orders

Where no criminal offence is being investigated, the government can still rely on courts to order journalists (and others) to disclose their sources – or grant access to their papers – in order to identify "wrongdoers".[137] Civil orders can compel disclosure of the identities of those who have acted in breach of confidence, and who thus constitute "wrongdoers". As such, where the Government is able, as it frequently is, to argue that a disclosure has occurred in breach of confidence, it has grounds upon which to apply for an order requiring journalists to disclose their sources. These mechanisms allow the Government to compel journalists to disclose their sources irrespective of whether the primary and secondary disclosures themselves are being pursued via the criminal or civil law.

5.3 Recent history of production orders

The recent history of production orders in cases of whistleblowers suggests that the police find it relatively easy to convince the judge at first instance to make the order, but that applications for judicial review of that decision are often successful, frequently on the basis that procedural errors have been committed. This has been the result in both ex parte Bright[138] and ex parte Moloney.[139]

5.3.1 Ex parte Bright - the use of PACE

In March 2000, Judge Stephens approved production orders against The Guardian and The Observer under s. 9 and sch. 1, para. 2 Police and Criminal Evidence Act 1984. These production orders were issued at the request of Special Branch for material held by The Observer and The Guardian newspapers relating to David Shayler. In particular Special Branch sought the original of a letter Mr Shayler wrote to The Guardian containing his email address. They also wanted the notes of Martin Bright, a journalist on The Observer who reported that Mr Shayler had named two MI6 officers involved in the alleged plot to kill Gaddafi.

---

[137] Norwich Pharmacal v Customs & Excise Commissioners [1974] AC 133, House of Lords
[138] R v Central Criminal Court, ex parte The Guardian, The Observer & Martin Bright, 21 July 2000
[139] R v Belfast County Court, ex parte Moloney, 27 October 1999

The orders were sought on the basis that they would advance police investigations into alleged breaches of the Official Secrets Act.[140] An appeal for judicial review of the decision against the Observer, ex parte Bright, was decided in July 2000. By a majority of two to one, the court quashed all the orders bar one. In each case, the basis for the decision was that the grounds for granting a production order (or access conditions) had not been met. Judge LJ emphasised the need for the presiding judge to be personally persuaded that each element of those conditions had been properly made out by the applicant police force.

In particular, the Court held that the evidence did not disclose a "serious arrestable offence" under the OSA. While s. 1(1) and s. 1(2) offences are always "arrestable", they become "serious arrestable" offences only if the disclosure in question has caused, was intended to cause, or was likely to cause serious harm to state security, or death or serious injury to any person.[141] In respect of the order sought against The Guardian, there was no credible claim that "serious" harm had been done (or was threatened) to national security. A more cogent case argument was presented in relation to The Observer, but again the access conditions were found not to have been properly made out.

Procedural errors in ex parte Bright

The appeal court found that the original grant of production orders against The Guardian and The Observer,[142] was marred by serious procedural errors. Amongst the most significant flaws were the following:

(i) All parties to the proceedings, including the judge, had assumed that any breach of the OSA amounted to a "serious arrestable" offence as defined by the Police and Criminal Evidence Act. In fact, OSA offences, whilst "arrestable", are not "serious arrestable" offences unless the disclosures have certain consequences (see above). The police were not put to proof on this crucial element of the application.

(ii) The task of giving evidence in support of the application was assigned to DS Flynn, a "qualified financial investigator", as required by police policy. However, DS Flynn had not been involved in the relevant investigation prior to this point. "In reality he knew nothing, or virtually nothing, about the case"[143] and was in no position to give an informed assessment of the value to the investigation of the materials in respect of which the orders were sought.

(iii) As a result of DS Flynn's lack of involvement with the investigation, all the evidence he produced for the court was hearsay. As such, it should have been

---

[140] Whether the Attorney-General would have consented to such a prosecution may never be known. Judge LJ expressed "considerable reservations whether there is any evidence at all that Mr. Bright can be said to have "disclosed" anything to anyone for the purposes of s. 5. On the other hand, Judge LJ suggested that he might legitimately have been pursued for inciting David Shayler to commit offences under s. 1 OSA R v Central Criminal Court, ex parte The Guardian, The Observer & Martin Bright, Divisional Court of Queen's Bench Division 21 July, draft judgment, p.16

[141] S. 116(6) PACE 1984

[142] The orders were granted on 17 March 2000 by His Honour Judge Martin Stephens QC at the Central Criminal Court

[143] R v Central Criminal Court, ex parte The Guardian, The Observer & Martin Bright, 21 July 2000, Divisional Court of Queen's Bench Division, draft judgment, p.12, per Judge LJ.

accorded less weight than it would have attracted if presented by a person with first-hand knowledge of the matters in question and capable of being fully cross-examined on the evidence.

(iv) Inspector Lerner – an officer more intimately involved in the case – attended the court throughout the hearing, but counsel for the defendants was not informed of this fact and so was not given the opportunity to cross-examine him. Counsel stated that he would, given the opportunity, wish to question Inspector Lerner. As the appeal court noted, "It is unfortunate that these observations did not lead to the obvious response that Mr. Lerner was indeed present and available at court."[144]

Comments on ex parte Bright

The judgment on appeal in the case was welcomed as "a ringing defence of press freedom and the newspapers' right to publish allegations by whistleblowers."[145] Closer examination of the judgment suggests that such enthusiasm is not warranted. In fact, the basis of the decision was primarily procedural errors, not the balancing of freedom of expression in the context of a national security interest. Indeed, "the police did not claim that either newspaper had in any way threatened national security."[146]

However, the judgment is promising in that it contains a recognition that government claims of national security need to be open to scrutiny. Judge LJ stated that judges "generally … cannot proceed on the basis of bare assertion by a police officer."[147] However, he also suggested that a "careful summary of the relevant factors" delivered in open court would suffice, unless even this level of disclosure would itself threaten national security, in which case "a procedure similar to that used in [Public Interest Immunity] applications" would be more appropriate.[148] It is arguable whether either of these two approaches can guarantee that the judge will be able to make a truly independent assessment of the claim that national security was under threat. However, Judge LJ emphasised that the presiding judge must be personally convinced that the relevant sch.1 factors are all satisfied and that he/she found unconvincing the Crown's assertion that it was "absolutely vital" for the police to get their hands on the material to facilitate prosecution of the case against David Shayler.

5.3.2 Ex parte Moloney - use of the PTA

In October 1999, a production order against Ed Moloney, a Northern Ireland journalist was quashed by the High Court in Belfast. A County Court order had been served on him directing him to surrender notes of interviews he carried out nearly ten years previously with William Stobie. The latter was a self-confessed police informer and alleged quartermaster of the Ulster Defence Association, a paramilitary organisation, who was being investigated for the 1989 murder of Pat Finucane, a Catholic solicitor. As in ex parte Bright, the judge found the access orders, in this case based on sch.7, para. 3(5) of the Prevention of Terrorism (Temporary Provisions) Act

[144] Ibid., p.13
[145] Richard Norton-Taylor, "Papers win Shayler MI5 case," The Guardian, 22 July 2000
[146] "A court comes to the rescue of free speech," The Guardian, 22 July 2000
[147] Draft judgment, p.13
[148] Ibid

1989 (which survive in sch. 5, para. 5 of the Terrorism Act 2000) were not made out, in particular as the police had not proved that there was a possibility that the notes would be of help in the investigation.[149]

Comment on ex parte Moloney

Despite this judgment, there is little reason to think that the agenda protecting freedom of expression has been significantly furthered as regards use of the PTA. As with s. 9 and sch. 1 PACE, there is no statutory requirement to weigh press freedom against the interests of facilitating a terrorist investigation, although the judge at first instance stated that he took the importance of a free press into account in making the order and this was accepted in judicial review by the High Court. Carswell LCJ took the view that – despite not being included as a statutory criterion – press freedom was a material factor to be considered, but the weight to be accorded to that factor was for the individual judge to determine.[150]

5.4 Conclusion

Even if the UK courts do consider there to be a presumption against making an order for disclosure, their historical reluctance to subject claims of national security to substantive scrutiny weakens its strength. Indeed, it continues to be disproportionately easy for an applicant able to plead national security to obtain an order for disclosure of sources. This concern is enhanced by recent legislative developments which further undermine protection for confidential sources. For example, the Terrorism Act 2000 ? which preserves the production order provisions from the Prevention of Terrorism (Temporary Provisions) Act 1989 – greatly extends the definitions of "terrorist" and "terrorism"[151] and the Regulation of Investigatory Powers Act 2000 provides a basis for email interception, a growing form of communication between journalists and their sources. In Liberty and ARTICLE 19's view, there is a clear need for stronger judicial scrutiny in the UK.

The traditional reluctance of the judiciary to pierce the veil of national security is unlikely to evaporate overnight, but these judgments may signal a change in attitude as the courts allocate more importance to protecting press freedom. It is notable for its insistence that even once access conditions have been made out, the decision to grant a production order is within the judge's discretion. In ex parte Bright, the Court held

---

[149] For detail on the background to this judgment, see Justice Delayed … Alleged State Collusion in the Murder of Patrick Finucane and Others, §6, British Irish Rights Watch, February 2000. <<http://www.fhit.org/birw/justice.html>>

[150] ex parte Moloney, draft judgment, p.15. The production order against Moloney was again quashed on the narrow ground that the statutory access conditions had not been properly satisfied by the applicant police force.

[151] S. 1 of the new Act defines terrorism in such a broad manner that it might encompass campaigning bodies, protesters and even workers involved in industrial disputes. The Act covers those who use or threaten action involving serious violence, serious property damage, endangerment of life, serious risks to public health and safety or serious interference with an electronic system. (s. 1(2) Terrorism Act 2000) The use or threat of such action becomes "terrorism" if designed to influence the government or intimidate (a section of) the public in the interests of a political, religious or ideological cause. (s. 1(1) Terrorism Act 2000) The Act also imposes a duty of disclosure on those – including journalists – who, in the course of their profession, obtain information relating to terrorist offences. (s. 19 Terrorism Act 2000) Those who, without reasonable excuse, fail to pass on such information to the police commit an offence

that in deciding how to exercise this discretion, the presiding judge should bear in mind that:

"[i]nconvenient or embarrassing revelations, whether for the Security Services or for public authorities, should not be suppressed. Legal proceedings [for production orders], or the threat of such proceedings, tends to inhibit discussion. … [C]ompelling evidence would normally be needed to demonstrate that the public interest would be served by such proceedings."[152]

In addition, the incorporation of the ECHR under the Human Rights Act 1998 will mean that courts are compelled to explicitly balance freedom of expression as a human right against claims in favour of disclosure. A presumption in favour of freedom of expression should mean that even where a source falls at the least protected end of the spectrum, the applicant seeking disclosure should be required to make a compelling case on the facts, to rebut a presumption that his application ought to fail.

Given that in the UK both criminal and civil forms of orders compelling source disclosure are discretionary, in all cases, the public interest in press freedom should be given considerable weight and a presumption against making the order should be observed. Judges should exercise their discretion to refuse such orders, save in exceptional cases, and only when they can be persuaded that the principle of journalistic confidence has genuinely to be abandoned in the public interest. Applicants claiming national security to be at stake should be put to proof on that matter. It is incumbent upon judges to question invocations of national security in support of those applications; to ensure that the applications are dealt with in a procedurally proper manner; to insist upon being furnished with carefully prepared and adequate evidence; and, ultimately, to accord free expression and the principle of journalistic confidence the weight they deserve.

[152] Draft judgment, p.27

6 Chilling the watchdogs and silencing the whistleblowers

The laws preventing primary and secondary disclosures of security-related information – whether through prosecution under the Official Secrets Act or through ex parte applications for interim injunctions – clearly affect those against whom they are deployed. They may ultimately lose their liberty and/or face substantial financial penalties. Similar consequences may be visited upon those who refuse to comply with statutory production orders or equitable disclosure orders under contempt of court provisions.

However, in addition to such "local" effects on those who disclose information and those who publish it, these mechanisms also produce wider or global chilling effects. Given the flawed DA-Notice system, the lack of adequate protection of sources, lack of clarity as to what national security covers and the lack of effective judicial oversight, the current regime is well poised to produce chilling effects on free expression.

There are two ways in which chilling effects dampen the free flow of information:

(i) confidential sources cease to make that information available for fear of the personal consequences of doing so; and

(ii) journalists and newspapers are reluctant to make secondary disclosures for fear of the personal and/or corporate consequences that may follow publication.

The greater the chilling effects at either level, the less the media are able to perform their vital role as watchdog of the democratic process, and the less informed the public are about matters they have an interest in knowing, and about which they have a right to know.

The European Court has stated that such chilling effects must be taken into account in determining whether a production order is compatible with Article 10 of the European Convention on Human Rights.[153] Individual cases can have indirect and wider consequences; and these should impact upon whether granting a given order can be regarded as "proportionate" in the sense demanded by the Article 10(2) requirement that any restriction on free expression be necessary in a democratic society. Given that democracy needs its watchdogs to be effective, the danger of producing such chilling effects must be given due weight in determining what the outcome of a given application ought to be.

6.1 Whistleblowers deterred

There can be little doubt that UK Governments have pursued a deliberate policy of seeking to chill at the first level, to make whistleblowers reluctant to come forward. This is supported by the judiciary's willingness to impose sentences under the OSA which signal a clear intention to exert a deterrent effect.[154] Given the extensive scope

[153] Goodwin v United Kingdom, 27 March 1996, 22 EHRR 123
[154] R v Tisdall (Sarah) (1984) 6 Cr.App.R.(S.) 155, Court of Appeal, Criminal Division

of the OSA offences and the lack of any public interest defence thereto, such deterrent effects must work to discourage the majority of disclosures which would otherwise be made in the public interest, as much as those who might seek to reveal information with malicious intent. For example, Jestyn Thirkell-White, a former colleague of David Shayler's who has recently come forward to endorse some of the latter's disclosures, "had always agreed with Shayler's analysis of MI5's failings … but was originally deterred, as well as appalled, by the harassment and the imprisonment of his former colleague."[155]

In the civil arena, the courts have recently expressed a willingness to treat breaches of contractual obligations of confidence by former members of the security and intelligence services as deserving of special treatment, in the form of particularly harsh and disproportionate penalties. In such cases, the courts have, for example, abandoned the general rule that the proper remedy for breach of contract is compensatory damages. Instead, they will at least consider awarding an account of profits, even where the disclosures in question cannot be regarded as having contravened any fiduciary duty of confidence.[156] At least part of the justification for this move is that the breach of contract in question in such cases will necessarily also constitute an offence under s. 1 OSA.[157] As such, this may be read as a further means of deterring acts in contravention of the OSA.

6.2 Media self-censorship

The recent trend of threatening journalists with prosecution under s. 5 OSA 1989 is being supplemented by a growing willingness to put financial pressure on newspapers via civil claims for damages.[158] If individual journalists cannot be made to fear for their liberty, then perhaps their employers can be made to fear for their wallets. Civil actions such as applications for interim injunctions and production orders often have indirect chilling effects as contesting such orders can be extremely expensive and time-consuming. In addition, failure to comply with their terms can result in fines and/or imprisonment. The authorities have some incentive in initiating proceedings – whether in the criminal or civil courts – because even a prosecution or suit that eventually fails can help reinforce the chill.

6.2.1 Slate - a case of Internet self-censorship

When David Shayler's allegations regarding MI6 involvement in a plot to assassinate Colonel Gaddafi were first circulated in 1998, the British newspapers hesitated in publishing the story for fear of being in breach of the standing injunction against disclosing any security-related information obtained from Shayler.[159]

Given the initial reluctance of British newspapers to publish Shayler's allegations about MI6 involvement in the Gaddafi plot, one UK-based journalist e-mailed an article about the allegation to Slate, an Internet news site. His suggestion was that Slate – being an American site – could publish the story which, given the global

---

[155] Mark Hollingsworth, "Opening the floodgates," The Guardian, 25 July 2000
[156] Attorney-General v Blake and Another, House of Lords, 27 July 2000
[157] Ibid., per Lord Nicholls of Birkenhead
[158] See §§4§6 for details regarding the range of claims brought against David Shayler and Associated Newspapers
[159] This was issued on 4 September 1997

nature of the Internet, would then be available in the UK.[160] Legal advice convinced Slate and its parent company, Microsoft, that the site would not necessarily escape sanction under the OSA and Slate therefore declined the invitation to publish. Shortly thereafter, The Sunday Times took the risk of mentioning Shayler's allegations and then other newspapers took up the story, reporting the fact that the allegations had been reported.[161] Had The Sunday Times not taken this step, the initial chill might have persisted. This illustrates how the threat of prosecution under the OSA can create chilling effects that reach beyond the borders of the UK.

On the other hand, if Slate had not been a subsidiary of a global corporation with a UK presence, it is unlikely that its editor would have felt the intended chill. "Our British friend instantly and effortlessly e-mailed us the rogue spy's article, and if we hadn't been worried about British law we would have made it as instantly and effortlessly available in Britain as if he'd published it himself."[162] This perhaps underlines the view expressed by Rear Admiral David Pulvertaft, former DA-Notice Secretary, that the Internet is "unpredictable and uncontrollable."[163] The government has sought to limit the impact of Internet publication by refusing to recognise dissemination over the Internet as putting the material in the public domain.[164] This view would mean that it was still prohibited to publish material from the Internet in newspapers, contrary to the general rule that once material is in the public domain, further publication does not threaten national security.

In the end it was the New York Times, which was not covered by the injunction, which published the details of the allegations in August 1998. The Guardian and then other British papers followed suit. The allegations were also the subject of an episode of the current affairs programme Panorama.

6.3 Conclusion

The chilling effect of UK legislation and practice extends far beyond those directly affected. Whether chilling effects are deliberately sought or whether instead they are the unintended by-products of actions taken for other reasons is to some extent irrelevant. As long as genuine whistleblowers are prosecuted alongside those who make genuinely damaging disclosures, and the media are actively prevented from publishing revelations of wrongdoing in the public interest, this chilling effect will be widely felt. The public interest demands a substantial thaw.

---

[160] Michael Kinsley, "How we lost that story," 8 August 1998 <<slate.msn.com/Readme/98-08-08/Readme.asp>>
[161] Ibid
[162] Ibid
[163] Quoted in "Internet exposure sparks fears for safety of spies," Financial Times, 13 May 1999
[164] David Pallister, "World web war worries censors," The Guardian, 13 May 1999

7 A culture of greater openness?

The British State has long been criticised for its culture of secrecy and lack of openness. The operation of the parliamentary system has been described as an elective dictatorship, and the stranglehold that the executive exercises on information and on decision-making was only tempered in the 1980s by the establishment of a select committee system.

The Labour Party, before its election in 1997, pledged that it would introduce a new culture of openness and transparency and broaden the processes of political accountability. Since it took office it has enacted one piece of legislation and has another in the pipeline, both of which – if they met international standards – would encourage and facilitate the dissemination of information to the media and the public.

The Public Interest Disclosure Act 1998 provides protection for leaks concerning unlawful or otherwise damaging activities, and its effects are already beginning to be felt. The Government is still attempting to steer its Freedom of Information Bill, providing for a right to access information held by public authorities, through the legislative process. However, it has come up against stiff resistance from many quarters, and it still falls far short of international standards[165] – in particular in relation to the excessive regime of exemptions included in the Bill.

While such legislation is welcome, neither piece of legislation applies to the Security and Intelligence services, illustrating the utter lack of willingness on the part of Government to tackle the veil of secrecy on matters of national security. It is precisely where other mechanisms of holding government and state to account are weakest that this new legislation is most feeble. The lack of accountability on matters concerning national security is further reinforced by inadequate parliamentary oversight on these matters.

7.1 Public Interest Disclosure Act 1998

The Public Interest Disclosure Act 1998 (PIDA) amends the Employment Rights Act 1996 to provide statutory protection for those who, in the public interest, breach duties of confidence and make disclosures regarding inter alia illegalities and wrongdoing.[166] Under certain conditions, PIDA will protect disclosures made to the press, although the preferred recipients of such disclosures are employers or those appointed to hear grievances.[167] Where individuals have made disclosures that fall within the scope of PIDA, they are entitled not to be subject to any adverse consequences as a result.[168] If they are dismissed as a result of making such disclosures, this will constitute unfair dismissal.[169]

The restricted scope of PIDA, however, highlights the limited way in which the Government is prepared to be open. None of these protections extends to those

[165] See Appendix 2
[166] S. 1 PIDA 1998, adding s. 43B ERA 1996
[167] S. 1 PIDA 1998, adding ss. 43C-43H ERA 1996
[168] S. 2 PIDA 1998, adding s. 47B ERA 1996
[169] S. 5 PIDA 1998, adding s. 103A ERA 1996

employed by the security and intelligence services,[170] even where they expose illegalities and incompetence. In light of the fact that the public interest may favour the disclosure of some secret information, this failure to offer protection would not appear to serve the public interest. Parliament ought to consider afresh the question of whether whistleblowers from within MI5 and MI6 should be given some protection against adverse consequences arising as a result of their disclosures. This is particularly important where, due to the lack of effective internal and external accountability structures, whistle-blowing may be the only way in which attention can be brought to bear on wrongdoing.

It might be said that the ability of those services to discharge their functions is peculiarly sensitive to the perceived loyalty and integrity of its officers. The courts have held that: "It is of paramount importance that members of the [Secret Intelligence Service] should have complete confidence in all their dealings with each other, and that those recruited as informers should have the like confidence."[171] However, it is surely going too far to suggest that this factor is of paramount importance. It may be that members of the Security and Intelligence Services should not benefit from exactly the same remedies as others, for example in relation to a right to reinstatement, but there can be little justification for denying such whistleblowers any protection from sanction.

7.2 The Freedom of Information Bill

The Government claims to honour a manifesto commitment by introducing a draft law on freedom of information. However, the Freedom of Information Bill currently going through Parliament fails to provide any alternative systematic means of disseminating security-related information which is in the public interest and so leaves the press-as-watchdog reliant on unauthorised disclosures.

The provisions in the Bill relating to security bodies effectively impose a blanket ban on any information about their operation.[172] MI5, MI6, GCHQ and the special forces, are completely excluded from the obligations of disclosure set out in the Bill.

In addition, all information "directly or indirectly supplied to the public authority by, or [which] relates to the work of" security bodies is also exempt (s. 21(1)). Moreover, a certificate signed by a Minister of the Crown will stand as conclusive evidence that any information requested falls within this blanket exemption.[173] A similar exemption applies in respect of other information to be withheld from the public in the interests of safeguarding national security. Again, a ministerial certificate will suffice as conclusive evidence that information falls within this category.[174] The provision for ministerial certificates to constitute conclusive evidence of a legitimate exemption offers scant comfort to those who regard the executive's ability to deflect proper scrutiny through claims of national security as a vital tool for maintaining the current imbalance between free expression and other elements of the public interest. Further

---

[170] S. 11 PIDA 1998, adding s. 193(4) ERA 1996
[171] Attorney-General v Blake and Another, 27 July 2000, House of Lords per Lord Nicholls of Birkenhead
[172] Submission to the UK Government on the Freedom of Information Bill, Censorship News No. 53, ARTICLE 19, July 1999
[173] cl.21(2) FOIB 2000
[174] cl.22 FOIB 2000

exemptions apply in respect of information that would be likely to prejudice defence, international relations, or the economic interests of the UK.[175]

Although s. 14 of the Bill allows authorities to disclose exempt information where this is in the public interest, the blanket nature of the security exemption is exacerbated by the fact it is one of only two exemptions to which s. 14 does not apply. Thus, s. 21 precludes disclosure of information even where this is clearly in the public interest. In effect, s. 21 completely negates any public access to the very broad range of information it covers. The Freedom of Information Bill therefore provides little more by access to information about national security than existed before.

7.3 Lack of democratic accountability of the Security and Intelligence Services

The need for greater accountability has led to some change in the way that the Security and Intelligence Services function. However, the extent to which they can be said to be subject to adequate parliamentary oversight is questionable. Yet parliamentary oversight is of key importance to ensuring that the security and intelligence services are accountable for their activities to the same degree as other public bodies. Judging by the number of whistleblowers that have come forth over time, and the support that they have attracted from some of their ex-colleagues, there appears to be a need for Parliament to scrutinise more closely the work of the security and intelligence services, particularly as internal mechanisms dealing with wrongdoing do not appear to be working.

Given the view of some ex-security and intelligence services officers that there is "no mechanism for internal dissent" and that members of MI5 have "no confidence in the so-called staff counsellor," a former permanent secretary,[176] whistle-blowing appears to some employees within the security and intelligence services as the only way to draw attention to wrongdoing. But relying on whistleblowing to expose wrongdoing is unsatisfactory and a poor substitute for properly effective structures of accountability, both internal and external.

In 1989 and again in 1994 there was some movement towards making the Security and Intelligence Services more accountable to elected representatives. In the wake of various leaks and controversies, and a case resulting from MI5?s surveillance of Liberty, the Government passed the 1989 Security Services Act which provides for statutory regulation of the activities of MI5.[177] GCHQ and MI6 were also formally established by the Intelligence Services Act 1994. However, the system of commissioners and tribunals empowered to "check the legality of warrants issued by ministers"[178] has yet to uphold a single complaint.

In 1994, the Intelligence Services Act was passed providing for limited Parliamentary oversight through the establishment of the Intelligence and Security Committee. However, limitations in its mandate have led many to conclude that the security and intelligence services are still not subject to a satisfactory level of Parliamentary

---

[175] cll.24, 25 & 27 FOIB 2000

[176] David Shayler and Jestyn Thirkell-White make these claims. See Mark Hollingsworth, "Opening the floodgates," The Guardian, 25 July 2000

[177] Hewitt and Harman vs. UK(1) (1991) 14 EHRR 657) European Court of Human Rights

[178] Ian Leigh, "Have you logged on to the MI5 website?" The Times, 29 August 2000

oversight.[179] In particular, as a statutory, rather than a Parliamentary Committee, it enjoys none of the formal powers of a Select Committee. Members are appointed by the Prime Minister, to whom it reports. Its remit is to examine expenditure, administration and policy of the security agencies, but it is restrained from examining operations. It can compel evidence from heads of agencies but has no power to summon witnesses or demand information from the public at large. Perhaps the most limiting feature of the Committee is the fact that it has to operate within the "ring of secrecy" – "the Committee cannot itself control the extent to which its conclusions are made public … the Prime Minister may – after consultation with the Committee – exclude material which he considers to be prejudicial to the continued discharge of the functions of the Agencies …"[180] This once again reinforces the executive's monopoly over defining what constitutes national security.

The view that the Intelligence and Security Committee should be given full Select Committee status was endorsed by the Home Affairs Select Committee last year and many other senior politicians before that.[181] This status would give the Committee a status independent of the executive in national security matters and would extend its ability to investigate wrongdoings and to maintain effective oversight over the Security and Intelligence Services. In proposing such a scheme in 1989, Roy Hattersley said:

"One of the advantages of a Select Committee in comparison with other institutions is that under our scheme it would write its reports after listening to the Government's advice about the need for security. That difference is crucial. It demonstrates the weakness of one and the strength of the other. It is the difference between keeping the supervision of the security services within the family of the establishment or extending it to a responsible but essentially independent oversight."[182]

Making the Security and Intelligence Services answerable to Parliament, in part by conferring full Select Committee status upon the Intelligence and Security Committee, would go some way to addressing the Security and Intelligence Services' current lack of accountability.

7.4 Conclusion

The lack of accountability and openness about the security forces makes whistleblowers from within the security and intelligence services particularly valuable. In the absence of any substantial alternative means by which Parliament can scrutinise the conduct of those services, unauthorised disclosures by those within the intelligence community constitutes a vital source of information on illegalities and wrongdoing. Yet the government has shown that it is not only unwilling to protect whistleblowers, but actually pursues them instead. Its commitment to openness is therefore open to question.

---

[179] "Our spies must answer to Parliament for their actions" Donald MacIntyre, The Independent, 22 August 2000
[180] Third Report: Accountability of the Security Services, Select Committee on Home Affairs, House of Commons, 21 June 1999
[181] Ibid
[182] Official Report 16 January 1989 col 37

ARTICLE 19 and Liberty believe that the Government can do much more to fulfil its commitment to openness. It should extend the protection offered by PIDA to its employees in the Security and Intelligence Services, and amend the current FOI Bill to remove the blanket exemption of security information and generally to meet the standards of openness of many other established democracies. Lastly, it should subject the Security and Intelligence Services to greater Parliamentary scrutiny than currently exists.

8 The Future of Secrecy under the Human Rights Act 1998

The most significant recent piece of legislation in relation to the laws on security and freedom of expression is the Human Rights Act 1998 (HRA) which came into force on 2 October 2000. The HRA finally incorporates the ECHR into UK law.[183] UK citizens are now able to rely on their ECHR rights before domestic courts, both as a defence to civil action and criminal prosecution and as a cause of action against public authorities in civil actions and judicial review.[184] The government regards the HRA as "a considerable achievement" and has "urged people to make the most of their new rights."[185]

For those facing prosecution and civil suits for making security-related disclosures such as David Shayler, Nigel Wylde, "Martin Ingrams", the HRA will be a welcome means of defending their right to free expression.

Under the HRA all legislation is to be construed, where possible, so as to render it compatible with the ECHR rights incorporated by this Act.[186] The HRA for the first time gives the courts in Scotland, Northern Ireland and England and Wales the power to strike out secondary legislation, such as statutory instruments and Orders in Council, where it does not admit of a compatible interpretation.[187] Similarly, the courts may invalidate administrative actions, including those conducted under the Royal Prerogative.[188] The courts cannot, however, strike out primary legislation – that is, Acts of Parliament.[189] Rather, in the name of parliamentary sovereignty, the courts will only be able to declare them incompatible with the ECHR[190] and it will then be for Parliament to amend the offending statute (the Act provides for a special "fast-track" procedure for this).[191] In the meantime, the incompatible statute will continue to apply, so a declaration of incompatibility has no impact on the proceedings within which it is issued.[192]

8.1 Freedom bred in the bone of common law?

It is sometimes claimed by the courts that the provisions of Article 10 of the ECHR are reflected in the common law of England and Wales,[193] and that freedom of

[183] The HRA does not incorporate Article 13, which confers the right to an effective remedy to correct infringements of the "substantive" ECHR rights
[184] Provided the individuals in question are "victims" of a breach of ECHR rights. See s. 7 Human Rights Act 1998
[185] Robert Verkaik, "Human rights claimants will be able to get instant justice," The Independent, 12 August 2000
[186] S. 3 HRA 1998
[187] Ibid
[188] S. 6 HRA 1998
[189] S. 3(2)(c) and s. 6(2)(a) HRA 1998
[190] S. 4 HRA 1998
[191] S. 10 HRA 1998
[192] S. 4(6) HRA 1998
[193] Derbyshire County Council v Times Newspapers Ltd [1993] AC 534; Attorney-General v Guardian Newspapers Ltd (No.2) [1988] 3 WLR 776

expression is “bred in the bone” of the common law.[194] However, ARTICLE 19 and Liberty believe that many aspects of British law and practice are not currently compatible with the ECHR. As a respected commentator has observed, "[the] British system precisely does not put the onus on government to justify interference with fundamental political rights. Parliamentary sovereignty in practice raises the executive above any systematic legal or political restraint. … Moreover, the judiciary imposes further restraints on itself, most notably in cases involving national security."[195] The HRA should, therefore, provide an opportunity for a significant review of British law and practice in the area of secrecy and national security.

One significant difference under the HRA is that courts will no longer be restricted to the standard of judicial review when assessing legislation and administrative actions. We believe that the courts should apply the three-part test set out above to any restrictions on freedom of expression, in particular to require any restriction to be "necessary in a democratic society". This means that the traditional deference courts have shown in the face of executive claims regarding national security is no longer acceptable; instead, courts should now see themselves as under a duty to subject attempts to limit free expression to proper scrutiny.

Another difference is that courts must now take account of the jurisprudence of the European Court and Commission of Human Rights.[196] Compliance with this requirement will demand that the UK courts interpret the "rights and freedoms guaranteed … consistent with the general spirit of the Convention."[197] This means that the courts should give a broad construction to the basic freedoms – as the right to free expression in Article 10(1) – construe the legitimate exceptions to those freedoms, such as the national security exemption in Article 10(2), in a narrow manner.

In this respect, it is worth citing statements made by the Lord Chancellor in a lecture delivered on 16 December 1997.[198] Discussing the likely impact of incorporating the ECHR, Lord Irvine of Lairg stated that from incorporation, judicial scrutiny:

> will not be limited to seeing if the words of an exception can be satisfied. The Court will need to be satisfied that the spirit of this exception is made out. It will need to be satisfied that the interference with the protected right is justified in the public interests in a free democratic society [and will] have to apply the Convention principle of proportionality.

8.2 An end to judicial deference

As noted above, the HRA should bring about a significant change in the way UK courts assess restrictions on freedom of expression on grounds of national security. It could be argued that the HRA requires courts to adopt an approach closer to that of

---

[194] R v Central Criminal Court, ex parte The Guardian, The Observer & Martin Bright, 21 July 2000, draft judgment, p.24

[195] F. Klug, K. Starmer and S. Weir, The Three Pillars of Liberty: Political Rights and Freedoms in the United Kingdom (1996), quoted in Michael Allen and Brian Thompson, Cases & Materials on Constitutional & Administrative Law, 5th edition, Blackstone Press, 1998, pp.507-508

[196] S. 2 HRA 1998

[197] Soering v United Kingdom (1989) 11 EHRR 439

[198] Lord Irvine of Lairg, “The Development of Human Rights in Britain under and Incorporated Convention on Human Rights,” partially reprinted in Michael Allen and Brian Thompson, Cases & Materials on Constitutional & Administrative Law, 5th edition, Blackstone Press, 1998, pp.539-541

the Special Immigration Appeals Commission, which was itself a response to a case in which the European Court concluded that, where questions of national security were at issue, the UK's immigration and deportation procedures were not ECHR-compliant.[199] As Lord Woolf MR has observed, subjecting claims regarding national security to proper scrutiny is not a role that the courts readily adopt in the absence of statutory intervention.[200] The HRA now provides that statutory basis and, as Lord Irvine of Lairg has concluded, "a more rigorous scrutiny than traditional judicial review will be required."[201]

The implications of a revised judicial approach could be wide-ranging. The HRA allows the courts to substantially reinterpret legislation, including the Official Secrets Act, and to issue declarations of incompatibility where this fails to render laws ECHR complaint. It also allows courts to re-evaluate the traditional approach towards the exercise of their discretion, for example in awarding production orders, interim injunctions and other civil remedies. Similarly, the deterrent effect of penalties can be taken into account by assessing whether a particular claim violates the requirement of proportionality.

8.3 The HRA and injunctions

The HRA contains specific provisions relating to interim injunctions which will significantly impede the Government's ability to secure gagging orders of this nature. Such injunctions are often obtained through an ex parte application, that is, in the absence of the respondent. Under the HRA, no ex parte relief can be granted unless either the government has taken all practicable steps to put the respondent on notice or there are compelling reasons for the proceedings to be conducted on this basis.[202] Moreover, an interim injunction will be justifiable only if the government can show that a permanent injunction is likely to be obtained at trial.[203] This is quite different from present requirements, under which the applicant only needs to show that there is an "arguable" case where the balance of convenience favours an injunction. Courts are now explicitly required to take into account the extent to which the material in question has entered or is about to enter the public domain and, significantly, the extent to which it would be in the public interest for the material to be published.[204]

These changes – inspired by media concern that the judiciary might give too little weight to freedom of expression as against individuals' right to privacy under Article 8 of the ECHR[205] – mean that ex parte interim injunctions to prevent security-related disclosures should now be far more difficult to obtain. They are much-needed safeguards against a remedy frequently abused by the Government to prevent the dissemination of a wide range of information.

---

[199] Chahal v United Kingdom (1997) 23 EHRR 413
[200] Secretary of State for the Home Department v Shafiq Ur Rehman, 23 May 2000
[201] Lord Irvine of Lairg, "The Development of Human Rights in Britain under and Incorporated Convention on Human Rights," partially reprinted in Michael Allen and Brian Thompson, Cases & Materials on Constitutional & Administrative Law, 5th edition, Blackstone Press, 1998, p.557
[202] S. 12(2) HRA 1998
[203] S. 12(3) HRA 1998
[204] S. 12(4)(a) HRA 1998
[205] Brian MacArthur, "Farewell kiss-and-tell," The Times, 18 August 2000

Section 12 Human Rights Act 1998 and Freedom of Expression

Section 12 (2) If the person against whom the application for relief is made ("the respondent") is neither present nor represented, no such relief is to be granted unless the court is satisfied-

(a) that the applicant has taken all practicable steps to notify the respondent; or

(b) that there are compelling reasons why the respondent should not be notified.

(3) No such relief is to be granted so as to restrain publication before trial unless the court is satisfied that the applicant is likely to establish that publication should not be allowed.

(4) The court must have particular regard to the importance of the Convention right to freedom of expression and, where the proceedings relate to material which the respondent claims, or which appears to the court, to be journalistic, literary or artistic material (or to conduct connected with such material), to-

(a) the extent to which-

(i) the material has, or is about to, become available to the public; or

(ii) it is, or would be, in the public interest for the material to be published;

(b) any relevant privacy code.

8.4 An ECHR-compliant OSA

The HRA should also significantly affect application of the Official Secrets Act. On the face of it, the OSA is clearly incompatible with the ECHR and is widely recognised to be so, although it remains to be seen as to whether the judiciary will necessarily agree with this view. The key issues here are whether it is possible to read the OSA in such a way that the various offences established by that Act are compatible with the ECHR; whether, if not, the courts will be willing to issue declarations of incompatibility; and finally, whether, in this case, the Government will be prepared to amend or repeal the offending provisions.

A disclosure under ss. 2-5 OSA 1989 is criminal only if it is “damaging”. In the view of Liberty and ARTICLE 19 this requirement can easily be read as including a broad public interest test. Under such an interpretation, damage would be construed broadly, so that it would refer not only to direct harm to national security but also to any benefits from a particular disclosure, for example in exposing wrongdoing. This interpretation is supported by s. 12(4)(a) HRA, dealing with injunctions, which explicitly requires that the broader public interest be taken into account, and by cases in which the ECHR has held that further dissemination of information already in the public zone may not be sanctioned.

A more difficult question is whether s. 1 OSA – the provision under which former members of the security and intelligence services may be prosecuted – can also be read in such a way as to be compatible with the ECHR. This offence does not contain any requirement of damage. However, it could be argued that by incorporating Article 10 into UK law, the HRA has implicitly amended the OSA so as to include

harm and public interest tests. Despite this, it may be worth noting that under the doctrine of the margin of appreciation, the European Court has always allowed States some latitude in protecting national security, and it remains unclear how the British courts will apply this doctrine.

Even if the courts do not read harm and public interest tests into s. 1 OSA, they still could, and indeed should, issue a declaration of incompatibility under the HRA, placing the onus on government to correct that incompatibility. However, since such a declaration does not affect the proceedings in which it is issued,[206] in theory the courts could jail a whistleblower under the OSA while at the same time recognising its incompatibility with the ECHR.

8.5 The HRA and civil claims

The HRA could also provide assistance to a genuine whistleblower facing the full range of civil claims that the government habitually deploys against those who make disclosures of security-related information. A public authority will only to be able benefit from civil remedies – including damages, account of profits and permanent injunctions – where they are ECHR-compliant, in the sense that they are necessary in a democratic society. Where the applicant is a true public actor, as opposed to a private one where the rules might be different, the same requirements of harm and public interest should apply. This should apply, for example, to claims by the Security and Intelligence Services for breach of confidence or contract. Unless these conditions are satisfied, granting the government a civil law remedy would not be a proportionate response to the disclosure.

8.6 Conclusion

The HRA requires UK courts to be more active in their scrutiny of restrictions on freedom of expression, including those justified in the name of national security. They should now assess whether such restrictions are necessary in a democratic society, rather than simply apply the weak standard of judicial review. This should mean that injunctions and other civil law remedies will be harder to obtain; production orders more difficult to justify; and convictions under the OSA restricted to a narrow range of genuinely damaging disclosures. ARTICLE 19 and Liberty see the incorporation of the ECHR into UK law through the HRA as an extremely positive development which provides an opportunity to redress the current striking imbalance between the right to freedom of expression and national security. We sincerely hope that the courts embrace this opportunity to bring about significant changes in the law.

[206] Laurence Lustgarten, "Freedom of Expression, Dissent, and National Security in the United Kingdom," in Sandra Coliver et al, Secrecy and Liberty: National Security, Freedom of Expression and Access to Information, Kluwer Law, 1999, p. 470

9 Recommendations

The protection of national security is a genuine and legitimate interest, not simply of the state or the government of the day, but of the public at large. However, as this report has shown, current law and practice in the UK signally fails to provide a proper balance between the public's right to freedom of expression and freedom of information and these national security interests. The law is overly restrictive, effectively precludes proper judicial oversight and encourages abuse.

Correcting the flaws of current law and practice – designing a structure able to deliver an appropriate balance between free expression and national security – demands a recognition of the fact that this is not a matter of weighing the interests of the state against the interests of its citizens. Ultimately, proper protection of the right to free expression will lead to more open, accountable and better government, as well as more appropriately-run, effective security services. This is in the overall interest of the State, as well as individuals, since both freedom of expression and national security are, ultimately, interests of the public. Balancing the two is a matter of determining how best to serve the overall public interest.

To the extent that judges in Britain have tended to adopt a "statist view of the public interest,"[207] they have failed to strike an appropriate balance between these two interests. Taking better account of citizens and their rights and of the corrective function of open government would aid in striking a better balance. The starting point for this balancing exercise has to be a presumption in favour of free expression, subject to narrowly-drawn restrictions which the authorities can justify as necessary to protect a legitimate aim. By explicitly incorporating a test of this sort, the Human Rights Act 1998 provides a unique opportunity to redress the imbalance that currently applies under British law and practice.[208]

To help provide a better balance between freedom of expression and national security in the United Kingdom, compatible with international standards in this area, Liberty and ARTICLE 19 make the following recommendations to the UK authorities:

Recommendation 1: Comprehensive Review of Existing Law

The government should immediately put in place a comprehensive process, including broad public consultations, to review all legislation and common law rules which restrict expression and information on grounds of national security. All such rules should be brought into line with the following recommendations.

Recommendation 2: Review of Ongoing Prosecutions and Convictions

The relevant authorities should immediately review all ongoing prosecutions and other legal measures which seek to justify restrictions on expression or information on

---

[207] Sydney Kentridge QC, "The Incorporation of the European Convention on Human Rights," quoted in Michael Allen and Brian Thompson, Cases & Materials on Constitutional & Administrative Law, 5th edition, Blackstone Press, 1998, p. 554

[208] Indeed, the change of perspective encouraged by the HRA may already be making itself felt, since "senior judges have been protecting free speech more strongly on the eve of the coming into force of the Human Rights Act 1998". Anthony Lester, "Finding common purpose," The Observer, 23 July 2000

grounds of national security. Where the applicable standards do not conform to these recommendations, the prosecution or other measure should be dropped. A similar review should be conducted in relation to any legal sanctions already applied, and redress should be provided as appropriate where either the sanctions themselves or the legal provisions under which they were imposed do not conform to these recommendations.

Recommendation 3: Judicial Scrutiny of all National Security Restrictions

Any restriction on expression or information on grounds of national security should be subject to a full appeal on the merits, and not just to judicial review, by the courts. Where the authorities claim that information cannot be revealed in open court, the remedy should be for the judicial authorities to review that information in camera, and not to deny effective access to the courts.

Recommendation 4: Clear Statutory Definition of National Security

All legislation posing restrictions on expression or information on grounds of national security should include a clear and narrow statutory definition of national security. Guidance in relation to such a definition can be found in Principle 2(a) of Johannesburg Principles, which reads as follows:

> A restriction sought to be justified on the ground of national security is not legitimate unless its genuine purpose and demonstrable effect is to protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government.

Recommendation 5: Burden of Proof to Rest with the Authorities

In all cases involving restrictions on expression or information on grounds of national security, those seeking to apply the restriction should bear the burden of proving that the restriction meets the standards outlined in these recommendations.

Recommendation 6: Three-part Test in European Convention to Apply

No restriction on expression or information on grounds of national security is legitimate unless it meets the following three-part test:

- it must be prescribed by law, in the sense that the law is accessible, unambiguous and narrowly and precisely drawn, and that individuals may foresee in advance whether a particular action is unlawful;
- its genuine purpose and demonstrable effect is to protect a legitimate national security interest; and
- it is necessary in a democratic society and, in particular:
  - (a) the expression or information at issue poses a serious threat to a legitimate national security interest;
  - (b) the restriction imposed is the least restrictive means possible for protecting that interest; and

(c) the harm to freedom of expression is not disproportionate to the benefits of the restriction in terms of protecting national security.

Recommendation 7: No Punishment without Damage: The Substantial Harm Test

No one should be subject to criminal penalty, including under the Official Secrets Act, for either a primary or a secondary disclosure of information unless that disclosure poses a real risk of substantial harm to a legitimate national security interest and there was a specific intention to cause harm of that sort. The following factors should be taken into account in assessing whether a particular disclosure meets this standard:

- whether the information has already entered, or is likely soon to enter, the public domain, including via the Internet; and
- whether there is an direct and immediate connection – a causal link – between the disclosure and the risk of harm.

Recommendation 8: A Public Interest Defence to Apply

All restrictions on expression and information on grounds of national security, whether criminal or civil, should be subject to a public interest defence so that sanction or liability should ensue only where any damage to national security is not outweighed by a corresponding public interest in disclosure.

Recommendation 9: Sanctions should not be Disproportionate

Any legal sanctions, criminal or civil, for breach of laws restricting expression or information on grounds of national security should not be so severe as to have a disproportionate effect on freedom of expression and information. In particular, in imposing sanctions, decision-makers should take account not only of the effect on the individual in breach, but also the wider chilling effect.

Recommendation 10: Limiting the Regime of Injunctions

The existing regime of injunctions should be limited in the following ways:

- ex parte interim injunctions should not be granted where they are not absolutely necessary and the applicant has not taken all practical steps to put the respondent on notice;
- the court should appoint a "special advocate" in all proceedings where an ex parte interim injunction is being sought;
- no interim injunction should be granted unless the applicant can show that he or she is likely, at trial on the merits, to succeed in obtaining an order restraining publication;
- in deciding whether to grant an injunction, judges should take into account the presumption in favour of the right to freedom of expression and information, and the severe impact of an injunction, as a form of prior restraint, on these rights;

- the grant of an injunction should be subject to a public interest test and, in particular, no injunction should be granted unless the benefits, in terms of avoiding harm to a legitimate national security interest, significantly and clearly outweigh the harm to freedom of expression;

- no injunction should be granted in respect of information already in the public domain, regardless of the means by which the information was disseminated, including via the Internet; and

- any decision to award an interim injunction should be subject to speedy review and there should be an opportunity for regular re-appraisal of any on-going injunction, interim or final.

Recommendation 11: Protection for Confidential Sources and Information

Journalists should not be required to reveal confidential sources or information unless there are exceptional circumstances, including an overriding public interest, in such a requirement. In particular, journalists should be able to withhold confidential sources or information unless the party seeking disclosure can show that it is necessary for the conduct of the defence of an accused person in a criminal trial or to the interest of society in criminal investigations. Necessity, in this context, implies the following:

- the material in question will materially assist the defence or criminal investigation;

- there is no alternative means by which the information might be obtained; and

- the public interest in disclosure significantly outweighs the harm to freedom of expression from disclosure.

Recommendation 12: The DA-Notice System should be Dismantled

The system as presently constituted should be dismantled. Any future security advisory system must be strictly voluntary and not a response to oppressive secrecy or other security laws. Where the press makes use of this system and receives an indication that no damage to national security is threatened by a given story, this outcome should be able to guarantee that there will be no subsequent adverse consequences as a result of publication.

Recommendation 13: Extension of statutory protection for whistleblowers

The Public Interest Disclosure Act 1998 should be amended so that it includes within its ambit security and intelligence personnel.

Recommendation 14: Accountability Mechanisms for the Security and Intelligence Services should be Enhanced

The Intelligence and Security Committee should be given full Select Committee status, including the right to review the operations of bodies falling within its mandate and the ability to decide on its own whether or not to publish its decisions.

APPENDIX 1

THE JOHANNESBURG PRINCIPLES ON NATIONAL SECURITY, FREEDOM OF EXPRESSION AND ACCESS TO INFORMATION

INTRODUCTION

These Principles were adopted on 1 October 1995 by a group of experts in international law, national security, and human rights convened by ARTICLE 19, the International Centre Against Censorship, in collaboration with the Centre for Applied Legal Studies of the University of the Witwatersrand, in Johannesburg.

The Principles are based on international and regional law and standards relating to the protection of human rights, evolving state practice (as reflected, inter alia, in judgments of national courts), and the general principles of law recognized by the community of nations.

These Principles acknowledge the enduring applicability of the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights and the Paris Minimum Standards of Human Rights Norms In a State of Emergency.[209]

PREAMBLE

The participants involved in drafting the present Principles:

Considering that, in accordance with the principles proclaimed in the Charter of the United Nations, recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world;

Convinced that it is essential, if people are not to be compelled to have recourse, as a last resort, to rebellion against tyranny and oppression, that human rights should be protected by the rule of law;

Reaffirming their belief that freedom of expression and freedom of information are vital to a democratic society and are essential for its progress and welfare and for the enjoyment of other human rights and fundamental freedoms;

Taking into account relevant provisions of the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the UN Convention on the Rights of the Child, the UN Basic Principles on the Independence of the Judiciary, the African Charter on Human and Peoples' Rights, the American Convention on Human Rights and the European Convention on Human Rights;

---

[209] The Siracusa Principles were adopted in May 1984 by a group of experts convened by the International Commission of Jurists, the International Association of Penal Law, the American Association for the International Commission of Jurists, the Urban Morgan Institute for Human Rights, and the International Institute of Higher Studies in Criminal Sciences. The Paris Minimum Standards were adopted in April 1984 by a group of experts under the auspices of the International Law Association

Keenly aware that some of the most serious violations of human rights and fundamental freedoms are justified by governments as necessary to protect national security;

Bearing in mind that it is imperative, if people are to be able to monitor the conduct of their government and to participate fully in a democratic society, that they have access to government-held information;

Desiring to promote a clear recognition of the limited scope of restrictions on freedom of expression and freedom of information that may be imposed in the interest of national security, so as to discourage governments from using the pretext of national security to place unjustified restrictions on the exercise of these freedoms;

Recognizing the necessity for legal protection of these freedoms by the enactment of laws drawn narrowly and with precision, and which ensure the essential requirements of the rule of law; and

Reiterating the need for judicial protection of these freedoms by independent courts;

Agree upon the following Principles, and recommend that appropriate bodies at the national, regional and international levels undertake steps to promote their widespread dissemination, acceptance and implementation:

I. GENERAL PRINCIPLES

Principle 1: Freedom of Opinion, Expression and Information

(a) Everyone has the right to hold opinions without interference.

(b) Everyone has the right to freedom of expression, which includes the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his or her choice.

(c) The exercise of the rights provided for in paragraph (b) may be subject to restrictions on specific grounds, as established in international law, including for the protection of national security.

(d) No restriction on freedom of expression or information on the ground of national security may be imposed unless the government can demonstrate that the restriction is prescribed by law and is necessary in a democratic society to protect a legitimate national security interest.[210] The burden of demonstrating the validity of the restriction rests with the government.

Principle 1.1: Prescribed by Law

---

[210] For the purposes of these Principles, a democratic society is one which has a government that is genuinely accountable to an entity or organ distinct from itself; genuine, periodic elections by universal and equal suffrage held by secret ballot that guarantee the free expression of the will of the electors; political groups that are free to organize in opposition to the government in office; and effective legal guarantees of fundamental rights enforced by an independent judiciary. This formulation is based on a definition of constitutionalism provided by Professor S A de Smith in The Commonwealth and its Constitution (London: Stevens & Sons, 1964), 106, augmented by reference to Article 25 of the International Covenant on Civil and Political Rights.

(a) Any restriction on expression or information must be prescribed by law. The law must be accessible, unambiguous, drawn narrowly and with precision so as to enable individuals to foresee whether a particular action is unlawful.

(b) The law should provide for adequate safeguards against abuse, including prompt, full and effective judicial scrutiny of the validity of the restriction by an independent court or tribunal.

Principle 1.2: Protection of a Legitimate National Security Interest

Any restriction on expression or information that a government seeks to justify on grounds of national security must have the genuine purpose and demonstrable effect of protecting a legitimate national security interest.

Principle 1.3: Necessary in a Democratic Society

To establish that a restriction on freedom of expression or information is necessary to protect a legitimate national security interest, a government must demonstrate that:

(a) the expression or information at issue poses a serious threat to a legitimate national security interest;

(b) the restriction imposed is the least restrictive means possible for protecting that interest; and

(c) the restriction is compatible with democratic principles.

Principle 2: Legitimate National Security Interest

(a) A restriction sought to be justified on the ground of national security is not legitimate unless its genuine purpose and demonstrable effect is to protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government.

(b) In particular, a restriction sought to be justified on the ground of national security is not legitimate if its genuine purpose or demonstrable effect is to protect interests unrelated to national security, including, for example, to protect a government from embarrassment or exposure of wrongdoing, or to conceal information about the functioning of its public institutions, or to entrench a particular ideology, or to suppress industrial unrest.

Principle 3: States of Emergency

In time of public emergency which threatens the life of the country and the existence of which is officially and lawfully proclaimed in accordance with both national and international law, a state may impose restrictions on freedom of expression and information but only to the extent strictly required by the exigencies of the situation and only when and for so long as they are not inconsistent with the government's other obligations under international law.

Principle 4: Prohibition of Discrimination

In no case may a restriction on freedom of expression or information, including on the ground of national security, involve discrimination based on race, colour, sex, language, religion, political or other opinion, national or social origin, nationality, property, birth or other status.

II. RESTRICTIONS ON FREEDOM OF EXPRESSION

Principle 5: Protection of Opinion

No one may be subjected to any sort of restraint, disadvantage or sanction because of his or her opinions or beliefs.

Principle 6: Expression That May Threaten National Security

Subject to Principles 15 and 16, expression may be punished as a threat to national security only if a government can demonstrate that:

(a) the expression is intended to incite imminent violence;

(b) it is likely to incite such violence; and

(c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.

Principle 7: Protected Expression

(a) Subject to Principles 15 and 16, the peaceful exercise of the right to freedom of expression shall not be considered a threat to national security or subjected to any restrictions or penalties. Expression which shall not constitute a threat to national security includes, but is not limited to, expression that:

(i) advocates non-violent change of government policy or the government itself;

(ii) constitutes criticism of, or insult to, the nation, the state or its symbols, the government, its agencies, or public officials,[211] or a foreign nation, state or its symbols, government, agencies or public officials;

(iii) constitutes objection, or advocacy of objection, on grounds of religion, conscience or belief, to military conscription or service, a particular conflict, or the threat or use of force to settle international disputes;

(iv) is directed at communicating information about alleged violations of international human rights standards or international humanitarian law.

(b) No one may be punished for criticizing or insulting the nation, the state or its symbols, the government, its agencies, or public officials, or a foreign nation, state or its symbols, government, agency or public official unless the criticism or insult was intended and likely to incite imminent violence.

Principle 8: Mere Publicity of Activities That May Threaten National Security

---

[211] "Public officials", for the purpose of these Principles, include the Head of State; the Head of Government; all government officials including Ministers; all officers of the military, security forces and police; and all people who hold elected office.

Expression may not be prevented or punished merely because it transmits information issued by or about an organization that a government has declared threatens national security or a related interest.

Principle 9: Use of a Minority or Other Language

Expression, whether written or oral, can never be prohibited on the ground that it is in a particular language, especially the language of a national minority.

Principle 10: Unlawful Interference With Expression by Third Parties

Governments are obliged to take reasonable measures to prevent private groups or individuals from interfering unlawfully with the peaceful exercise of freedom of expression, even where the expression is critical of the government or its policies. In particular, governments are obliged to condemn unlawful actions aimed at silencing freedom of expression, and to investigate and bring to justice those responsible.

III. RESTRICTIONS ON FREEDOM OF INFORMATION

Principle 11: General Rule on Access to Information

Everyone has the right to obtain information from public authorities, including information relating to national security. No restriction on this right may be imposed on the ground of national security unless the government can demonstrate that the restriction is prescribed by law and is necessary in a democratic society to protect a legitimate national security interest.

Principle 12: Narrow Designation of Security Exemption

A state may not categorically deny access to all information related to national security, but must designate in law only those specific and narrow categories of information that it is necessary to withhold in order to protect a legitimate national security interest.

Principle 13: Public Interest in Disclosure

In all laws and decisions concerning the right to obtain information, the public interest in knowing the information shall be a primary consideration.

Principle 14: Right to Independent Review of Denial of Information

The state is obliged to adopt appropriate measures to give effect to the right to obtain information. These measures shall require the authorities, if they deny a request for information, to specify their reasons for doing so in writing and as soon as reasonably possible; and shall provide for a right of review of the merits and the validity of the denial by an independent authority, including some form of judicial review of the legality of the denial. The reviewing authority must have the right to examine the information withheld.[212]

Principle 15: General Rule on Disclosure of Secret Information

[212] Additional grounds for obtaining and correcting personal information in files about oneself, such as the right to privacy, lie beyond the scope of these Principles.

No person may be punished on national security grounds for disclosure of information if (1) the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or (2) the public interest in knowing the information outweighs the harm from disclosure.

Principle 16: Information Obtained Through Public Service

No person may be subjected to any detriment on national security grounds for disclosing information that he or she learned by virtue of government service if the public interest in knowing the information outweighs the harm from disclosure.

Principle 17: Information in the Public Domain

Once information has been made generally available, by whatever means, whether or not lawful, any justification for trying to stop further publication will be overridden by the public's right to know.

Principle 18: Protection of Journalists' Sources

Protection of national security may not be used as a reason to compel a journalist to reveal a confidential source.

Principle 19: Access to Restricted Areas

Any restriction on the free flow of information may not be of such a nature as to thwart the purposes of human rights and humanitarian law. In particular, governments may not prevent journalists or representatives of intergovernmental or non-governmental organizations with a mandate to monitor adherence to human rights or humanitarian standards from entering areas where there are reasonable grounds to believe that violations of human rights or humanitarian law are being, or have been, committed. Governments may not exclude journalists or representatives of such organizations from areas that are experiencing violence or armed conflict except where their presence would pose a clear risk to the safety of others.

IV. RULE OF LAW AND OTHER MATTERS

Principle 20: General Rule of Law Protections

Any person accused of a security-related crime[213] involving expression or information is entitled to all of the rule of law protections that are part of international law. These include, but are not limited to, the following rights:

(a) the right to be presumed innocent;

(b) the right not to be arbitrarily detained;

(c) the right to be informed promptly in a language the person can understand of the charges and the supporting evidence against him or her;

(d) the right to prompt access to counsel of choice;

(e) the right to a trial within a reasonable time;

[213] For the purposes of these Principles, a "security-related crime" is an act or omission which the government claims must be punished in order to protect national security or a closely related interest.

(f) the right to have adequate time to prepare his or her defence;

(g) the right to a fair and public trial by an independent and impartial court or tribunal;

(h) the right to examine prosecution witnesses;

(i) the right not to have evidence introduced at trial unless it has been disclosed to the accused and he or she has had an opportunity to rebut it; and

(j) the right to appeal to an independent court or tribunal with power to review the decision on law and facts and set it aside.

Principle 21: Remedies

All remedies, including special ones, such as habeas corpus or amparo, shall be available to persons charged with security-related crimes, including during public emergencies which threaten the life of the country, as defined in Principle 3.

Principle 22: Right to Trial by an Independent Tribunal

(a) At the option of the accused, a criminal prosecution of a security-related crime should be tried by a jury where that institution exists or else by judges who are genuinely independent. The trial of persons accused of security-related crimes by judges without security of tenure constitutes a prima facie violation of the right to be tried by an independent tribunal.

(b) In no case may a civilian be tried for a security-related crime by a military court or tribunal.

(c) In no case may a civilian or member of the military be tried by an ad hoc or specially constituted national court or tribunal.

Principle 23: Prior Censorship

Expression shall not be subject to prior censorship in the interest of protecting national security, except in time of public emergency which threatens the life of the country under the conditions stated in Principle 3.

Principle 24: Disproportionate Punishments

A person, media outlet, political or other organization may not be subject to such sanctions, restraints or penalties for a security-related crime involving freedom of expression or information that are disproportionate to the seriousness of the actual crime.

Principle 25: Relation of These Principles to Other Standards

Nothing in these Principles may be interpreted as restricting or limiting any human rights or freedoms recognized in international, regional or national law or standards.

The following experts participated in the Consultation that drafted these Principles in their personal capacity. Organizations and affiliations are listed for purposes of identification only.

Laurel Angus, Executive Director, Centre for Applied Legal Studies, University of the Witwatersrand, South Africa

Lawrence W Beer, Professor of Civil Rights, Department of Government and Law, Lafayette College, USA

Geoffrey Bindman, solicitor, Bindman and Partners, London, UK

Dana Briskman, Legal Director, Association for Civil Rights, Israel

Richard Carver, Africa Programme Consultant, ARTICLE 19, London, UK

Yong-Whan Cho, Duksu Law Offices, Seoul, South Korea

Sandra Coliver, Law Programme Director, ARTICLE 19, Washington DC, USA

Peter Danowsky, Danowsky & Partners, Stockholm, Sweden

Emmanuel Derieux, Professor of Media Law, University of Paris 2, and Co-editor, Legipresse, Paris, France

Frances D'Souza, Executive Director, ARTICLE 19, London, UK

Elizabeth Evatt AC, member, UN Human Rights Committee and legal consultant, Sydney, Australia

Felipe Gonzalez, Professor of Law, Diego Portales University, Santiago, Chile and Legal Officer for Latin America, International Human Rights Law Group, Washington DC

Paul Hoffman (Conference Chair), media lawyer, Los Angeles, USA

Gitobu Imanyara, Advocate of the High Court of Kenya, and Editor-in-Chief, Nairobi Law Monthly, Kenya

Lene Johannessen, Media Project, Centre for Applied Legal Studies, University of the Witwatersrand, Johannesburg, South Africa

Raymond Louw, Chairman, Freedom of Expression Institute, Johannesburg, South Africa

Laurence Lustgarten, Professor of Law, University of Southampton, UK

Paul Mahoney, Deputy Registrar, European Court of Human Rights, Council of Europe[214]

Gilbert Marcus, Advocate of the Supreme Court of South Africa, Johannesburg, South Africa

Kate Martin, Executive Director, Center for National Security Studies, Washington DC, USA

Juan E Mendez, General Counsel, Human Rights Watch, New York, USA

[214] Because of his position as an international civil servant, Mr Mahoney did not endorse or oppose these Principles

APPENDIX 2

Summary of recommendations in ARTICLE 19's publication, The Public's Right to Know: Principles on Freedom of Information Legislation (ARTICLE 19, June 1999).

PREFACE

Information is the oxygen of democracy. If people do not know what is happening in their society, if the actions of those who rule them are hidden, then they cannot take a meaningful part in the affairs of that society. But information is not just a necessity for people, it is an essential part of good government. Bad government needs secrecy to survive. It allows inefficiency, wastefulness and corruption to thrive. As Amartya Sen, the Nobel Prize-winning economist has observed, there has never been a substantial famine in a country with a democratic form of government and a relatively free press. Information allows people to scrutinise the actions of a government and is the basis for proper, informed debate of those actions.

Most governments, however, prefer to conduct their business in secret. In Swahili, one of the words for government means "fierce secret". Even democratic governments would rather conduct the bulk of their business away from the eyes of the public. And governments can always find reasons for maintaining secrecy – the interests of national security, public order and the wider public interest are a few examples. Too often governments treat official information as their property, rather than something which they hold and maintain on behalf of the people.

That is why ARTICLE 19 has produced this set of international principles – to set a standard against which anyone can measure whether domestic laws genuinely permit access to official information. They set out clearly and precisely the ways in which governments can achieve maximum openness, in line with the best international standards and practice.

Principles are important as standards but on their own they are not enough. They need to be used – by campaigners, by lawyers, by elected representatives and by public officials. They need applying in the particular circumstances that face each society, by people who understand their importance and are committed to transparency in government. We publish these principles as a contribution to improving governance and accountability and strengthening democracy across the world.

BACKGROUND

These Principles set out standards for national and international regimes which give effect to the right to freedom of information. They are designed primarily for national legislation on freedom of information or access to official information but are equally applicable to information held by inter-governmental bodies such as the United Nations and the European Union.

The Principles are based on international and regional law and standards, evolving state practice (as reflected, inter alia, in national laws and judgments of national courts) and the general principles of law recognised by the community of nations.

They are the product of a long process of study, analysis and consultation overseen by ARTICLE 19, drawing on extensive experience and work with partner organisations in many countries around the world.

PRINCIPLE 1. MAXIMUM DISCLOSURE

Freedom of information legislation should by guided by the principle of maximum disclosure

PRINCIPLE 2. OBLIGATION TO PUBLISH

Public bodies should be under an obligation to publish key information

PRINCIPLE 3. PROMOTION OF OPEN GOVERNMENT

Public bodies must actively promote open government

PRINCIPLE 4. LIMITED SCOPE OF EXCEPTIONS

Exceptions should be clearly and narrowly drawn and subject to strict "harm" and "public interest" tests

PRINCIPLE 5. PROCESSES TO FACILITATE ACCESS

Requests for information should be processed rapidly and fairly and an independent review of any refusals should be available

PRINCIPLE 6. COSTS

Individuals should not be deterred from making requests for information by excessive costs

PRINCIPLE 7. OPEN MEETINGS

Meetings of public bodies should be open to the public

PRINCIPLE 8. DISCLOSURE TAKES PRECEDENCE

Laws which are inconsistent with the principle of maximum disclosure should be amended or repealed

PRINCIPLE 9. PROTECTION FOR WHISTLEBLOWERS

Individuals who release information on wrongdoing – whistleblowers – must be protected