NATIONAL SECURITY AND OPEN GOVERNMENT:

STRIKING THE RIGHT BALANCE

NATIONAL SECURITY AND OPEN GOVERNMENT:

STRIKING THE RIGHT BALANCE

Campbell Public Affairs Institute
The Maxwell School of Syracuse University

Commentaries edited by the Campbell Public Affairs Institute from a Symposium co-organized with the Open Society Justice Initiative.

The Maxwell School of Syracuse University

First Edition 2003

Library of Congress Cataloging-in-Publication Data
National security and open government : striking the right balance.-- 1st ed.
p. cm.
ISBN 0-9720512-2-8
1. National security. 2. Transparency in government. 3. Freedom of information. I. Campbell Public Affairs Institute. II. Title.
UA10.5.N276 2003
355'.03--dc22

2003014657

Printed in Syracuse, New York
United States

TABLE OF CONTENTS

PREFACE

Alasdair Roberts
Director
Campbell Public Affairs Institute

The rapid diffusion of "right to information laws" around the world in the last decade might seem to give hope that we are entering a new era of governmental openness.

The realities are more complex. Many governments continue to resist demands for transparency in areas of government that are thought to touch on matters of national security. Right to information laws often give governments broad and often unchecked discretion to withhold information in the name of national security.

The terror attacks of September 11, 2001 have also compelled a reappraisal of the balance that should be struck between the interests served by governmental openness, and the need to protect national security -- in the United States, and many other countries as well.

The eight commentaries in this book -- all written in the early months of 2003 -- describe how governments around the world have reconciled calls for openness and concern for the preservation of national security. They also consider how the balance between transparency and national security should be struck.

They also ask whether the basic premise -- that there is a tension between openness and security -- should be taken for granted. In many cases -- perhaps more than we initially imagine -- transparency and security may run together. Openness provides citizens with information about their community's vulnerabilities, and arms them with the knowledge needed to prevent harm being done.

The commentaries included in this book were prepared for a symposium on National Security and Open Government held in Washington, DC on May 5, 2003. The symposium was a jointly run project of the Campbell Public Affairs Institute and the Open Society Justice Initiative.

The Campbell Institute is a research center within the Maxwell School of Citizenship and Public Affairs of Syracuse University. The Institute's aim is to promote better understanding of contemporary challenges in democratic governance.

The Institute is named in honor of Alan K. Campbell, Dean of the Maxwell School from 1969 to 1976. "Scotty" Campbell had a distinguished career in academia, state and federal government, and the private sector. Through its work, the Institute honors his lifelong commitment to effective government; full and equal citizen participation; and incisive, policy-relevant research.

The Open Society Justice Initiative is an operational arm of the Open Society Institute that promotes rights-based law reform, builds knowledge and strengthens legal capacity worldwide. The Justice Initiative works in the fields of national criminal justice reform; international justice; freedom of information and expression; anticorruption; and equality and citizenship. Its offices are in New York, Budapest, and Abuja; its Executive Director is James A. Goldston. Support for this project was provided through the Justice Initiative's Freedom of Information and Expression Program, which is headed by Senior Program Manager Helen Darbishire.

This project was undertaken with the hope that it would help to advance dialogue about one of the most important and difficult subjects confronting advocates and researchers interested in governmental openness. This book can also be downloaded from the Campbell Institute's website, http://www.campbellinstitute.org.

The Institute is grateful to the contributors for their commitment to this project. Many traveled long distances to participate in our Washington meeting. They persevered despite the uncertainties and complications caused by the commencement of the second Gulf war a few weeks before our May 5 meeting.

The success of the symposium is largely due to the skill and effort of Bethany Walawender, Assistant Director of the Institute, and Kelley Coleman, the Institute's Office Coordinator. Production of this book was led by Bethany Walawender with the assistance of our editor, Alyssa Colonna.

The Institute is grateful to Helen Darbishire for her support and advice in the development of this project. Thanks are also due to Ann Florini, Senior Fellow in the Governance Studies program of the Brookings Institution, who acted as host for our Washington meeting; and to Andrew Eggers, who managed arrangements at the Brookings Institution.

Finally, we wish to acknowledge the contribution of three individuals who served as chairs or panelists for the May 5 meeting, but did not write papers for this volume: Ulf Öberg, a lawyer currently completing his doctoral studies at the Faculty of Law of Stockholm University; Professor William Banks of the Syracuse University College of Law; and Kevin O'Connell, Director of the RAND Intelligence Policy Center.

We appreciate your comments on this book. Other books and comments published by the Institute can also be downloaded from our website. Our e-mail address is info@campbellinstitute.org.

Helen Darbishire
Senior Program Manager
Open Society Justice Initiative

International law defines national security as a legitimate restriction on freedom of expression and information and many national laws define further how it should be applied, and yet it remains one of the most problematic restrictions because it is regularly overused and abused in ways which seem to contravene international standards. The debate about what are appropriate applications of the national security exemption has taken on a sharper focus in recent years, in part because of the adoption of many new FOI laws around the globe — 35 in the past 10 years — and in part in the wake of September 11, particularly as the United States is often referred to as the benchmark in setting national security standards.

One of the biggest problems facing human rights activists is that national security is still relatively loosely defined and open to interpretation. The best attempt at a universal definition of national security was the development of Johannesburg Principles in 1995 by a group of lawyers, academics and human rights activists. As Toby Mendel of Article 19 describes in his paper, these principles do not create new standards but distill existing standards from international and comparative law. Useful as they are in narrowing the scope of national security, the Johannesburg Principles do not contain a precise definition of what information it is or is not legitimate to withhold from the public on grounds of national security, and supplementary guiding principles are clearly needed.

The papers contained in this publication were written for a meeting convened in Washington in May 2003 by the Open Society Justice Initiative and the Campbell Public Affairs Institute of Syracuse University. The meeting, hosted by the Brookings Institution, brought together about 30 people concerned from one perspective or another about the issue of national security, including non-governmental organizations, academics, and members of government. The aim of the meeting was to discuss how national security is impacting on the rights to freedom of expression and information at the beginning of the 21st Century. The aim was also to define priorities for future work in the area of promoting free speech and open government, including the types of projects in which the Justice Initiative and other parts of the Open Society Institute should engage.

The problems caused by lack of definitions are all too evident in the UK: as John Wadham and Kavati Modi of Liberty (UK) point out in their paper, the appallingly broad definition of threats to national security in Britain, which the courts have stated is a matter for the executive to assess, effectively blocks legal challenges to denials of access to information. As other contributors note, government secrecy masks incompetence and provides the perfect cover for wrongdoing; a quick review of the historical record shows that many of the most contentious secrecy cases in the US, Europe, and elsewhere, were in fact more about hiding government malfeasance than protecting against genuine menaces to the nation. In an era when corruption is one of the greatest threats to the development of democracy, the danger is that secrecy — whether justified by national security or privacy or commercial confidentiality — will permit corruption to flourish. In addition to helping expose and combat corruption, it was noted that openness could prove to be one of the most powerful forces in the war against terrorism: a well-informed public can be alert to risks and can often identify shortcomings in security structures better than those within the security apparatus.

One of the dilemmas discussed at the meeting was the issue of the "balancing test". Under international law and the national law of many states, the legitimate exemption of national security must be balanced against the public interest inherent in protecting the fundamental right to expression and information. In his provocative paper for the conference, Tom Blanton of the National Security Archive challenges this construction, arguing that it is inappropriate to balance open government, which is both a condition and a value of democratic societies, against national security, which is not a value in itself but rather a condition that allows a nation to maintain and protect its values. Other contributors to the discussion echoed this, questioning how one can talk about balancing a right (freedom of expression and information) against something which is not a right (national security). In balancing rights one starts with two things which are prima facie equal and have to be given equal weight at the outset. With national security one is not talking about a right, but a restriction which has to be interpreted in a limited way. The problem, as another discussant noted, is that national security has become an overweight, even obese, beast which urgently needs to be put on a diet if one is to protect fundamental human rights from its crushing bulk. The proposal was not to shoot this beast but rather to slim it down.

Many of the main threads of the debate at the Brookings Institution in May are to be found in the papers presented here. The impact of national security classification on the right of access to government-held information, a right newly-secured in law in many countries, was a predominant theme, but the impact of national security on freedom of expression and media freedom was also a cause for concern. Many countries have laws which provide criminal sanctions for expression which is deemed to jeopardize national security. As Felipe González notes in his paper, the desacato laws of many Latin American countries, laws which criminalize contempt of authority, have the alleged objective of protecting state security and public order. Like sedition laws around the world, these provisions date back to colonial times and are based on anachronistic legal and political concepts which should not be justified by modern definitions of the need to protect national security. Once again, it seems that the national security paradigm needs revisiting.

The debate on moving beyond the balancing test does not, however,

adequately define the issues in many developing democracies. Rather, in countries such as Bulgaria and Indonesia, the challenge can at times be even to reach the balancing test: in these countries much information remains outside the scope of freedom of information laws, falling under blanket national security exemptions which preclude documents from consideration of release by public officials, and often make them inaccessible even to judges and certainly to the plaintiff's lawyers in appeal hearings. The papers by Alexander Kashumov of the Access to Information Program (Bulgaria) and Bimo Nugroho of the Institute for Studies on the Free Flow of Information (Indonesia) address these and related problems in transitional democracies.

Another way in which the balancing test is not even reached is that information is exempted because it relates to international relations as mediated by inter-governmental organizations (IGOs), either on grounds that release will harm international relations or on the principle of originator control, which determines that the country which created the information should decide whether or not it should be made public. A prime example of this is information which has been shared with NATO by one state and cannot be obtained through FOI requests in other states which hold the information. The originator control classification system within NATO leads to problems with information generated by the NATO secretariat itself, including, ironically, the procedures by which NATO information is classified – themselves contained in a restricted document which non-governmental organizations (NGOs) have tried and failed to obtain. Other inter-governmental bodies such as the European Union and international financial institutions such as the World Bank, have similar classification policies which can make information access difficult. Advocates often feel that they are running in circles as they are passed from national government to IGO and back again in their efforts to get access to documents. The paper by Alasdair Roberts of the Campbell Public Affairs Institute addresses these issues and looks at how the widespread introduction of FOI laws in Central and Eastern Europe has been followed by the passage of national security legislation, with governments commonly citing NATO membership requirements as the justification.

In spite of all these challenges, many of the participants in the Justice Initiative-Campbell Institute meeting declared themselves to be optimistic about the future of open government and free speech. It was with

enthusiasm that participants considered priorities for follow-up work, proposing how to demonstrate more clearly the need to redefine and even re-conceptualize national security, how to show that openness can be as much of an ally in the war against terrorism as secrecy, how better to harness the anti-corruption movement to drive transparency, how to encourage and protect whistleblowers, and how to make use of best practices, legislation and litigation to set the highest standards for application of the national security restriction. The Open Society Justice Initiative will be engaged in these future initiatives as part of its commitment to promoting open societies. In the meantime, we very much hope that this publication will serve to further the debate and contribute to a deeper understanding of how national security does and should relate to the fundamental rights to freedom of expression and information.

CONTRIBUTORS

Thomas S. Blanton is Director of the National Security Archive at George Washington University in Washington D.C. Blanton served as the Archive's first Director of Planning & Research beginning in 1986, became Deputy Director in 1989, and Executive Director in 1992. He wrote *White House E-Mail: The Top Secret Computer Messages the Reagan-Bush White House Tried to Destroy* (The New Press, 1995); co-authored *The Chronology* (New York: Warner Books, 1987, 687 pp.) on the Iran-contra affair; and served as a contributing author to three editions of the ACLU's authoritative guide, *Litigation Under the Federal Open Government Laws*, and to the Brookings Institution study *Atomic Audit: The Costs and Consequences of U.S. Nuclear Weapons Since 1940* (Washington, D.C.: Brookings, 1998). His articles have appeared in *The International Herald-Tribune*, *The New York Times*, *The Washington Post*, *Los Angeles Times*, *The Wall Street Journal*, *The Boston Globe*, *Slate*, the *Wilson Quarterly*, and many other publications. A graduate of Harvard University, where he was an editor of the independent university daily newspaper *The Harvard Crimson*, he won Harvard's 1979 Newcomen Prize in history. He also received the 1996 American Library Association James Madison Award Citation for "defending the public's right to know." He is a founding editorial board member of *freedominfo.org*, the virtual network of international freedom of information advocates.

Deirdre Curtin is a Professor of International and European Governance at the Utrecht School of Governance, University of Utrecht. She is a member of the Dutch Academy of Science (KNAW) and Vice-Chairperson of the Standing Committee of Experts on Matters relating to International Immigration, Refugee and Criminal Law in the Netherlands. Her publications include *Irish Employment Equality Law* (1989), *Postnational Democracy: The European Union in Search of a Political Philosophy* (Kluwer, 1997), and numerous articles on subjects relating to the constitutional and institutional development of the European Union, the principles of open government and democratic participation as well as human rights protection.

Helen Darbishire is Senior Program Manager at the Open Society Justice Initiative where she is responsible for the Freedom of Information and Expression Program. A human rights advocate specializing the right to freedom of expression and information, Helen has worked with the Open Society Institute (Soros Foundation) since 1999, and before that with Article 19 (1989-1998); she has also been a consultant on media freedom and freedom of information issues for a number of NGOs and IGOs. She has worked on the development of many of recent freedom of information laws, and was one of the drafters of the Bosnian freedom of information law. She is author of numerous reports on freedom of information media and media freedom, including NGOs and Information Interventions, in *Forging Peace* (Edinburgh University Press, 2002), "The Media in Transition," in *Central and Southeastern Europe in Transition* (Preager, 2000) *Media and Elections in Media and Democracy Handbook*, (Council of Europe, 1998), *Critical Analysis of Media Legislation in Europe* (UNESCO, September 1997).

Felipe González is a Professor of International Human Rights Law and Constitutional Law at the University Diego Portales Law School in Santiago, Chile. He is also the Director of the Chilean Forum for Freedom of Expression (an organization from the civil society) and of a Latin American network of Human Rights Legal Clinics. He has been a representative in Latin America for the International Human Rights Law Group since 1991. He has been a Tinker Visiting Professor at the University of Wisconsin Law School (2000) and a Visiting Professor at American University in Washington, D.C. (2001 and 2002). He participated in the preparation of the *Johannesburg Principles on National Security and Access to Information*, and has written extensively on this matter, including the book *Protección Democrática de la Seguridad Interior* (*Democratic Protection of Internal Security, 1991*) and *Leyes de Desacato y Libertad de Expresión* (*Contempt Laws and Freedom of Expression*, 2000). He has litigated in many cases on freedom of expression issues before the Inter-American Commission on Human Rights, including a current one challenging the censorship of a book by local Chilean tribunals.

Alexander Kashumov is a human rights lawyer and head of the legal team of the Access to Information Programme (AIP), a non-governmental organization based in Sofia, Bulgaria. He has worked AIP since 1997 and has litigated before national courts in about fifty FOI and other human rights cases. He also takes part in the advocacy and monitoring activities

of AIP, writing comments and reports on FOI, national security exemptions and personal data protection legislation and practices. He has also provided FOI training for non-governmental organizations, journalists and public officials, and campaigned for better FOI and human rights legislation. He has two masters degrees, in Law and Philosophy.

Jonathan Klaaren is a Professor at the School of Law of the University of the Witwatersrand in Johannesburg, South Africa. He is Co-Director of the School's Research Unit on Law and Administration (RULA). Together with Iain Currie, he is the author of *The Promotion of Access to Information Act Benchbook* (2002), the leading legal commentary on this new legislation in South Africa. He is also an editor of *Constitutional Law of South Africa*. Mr. Klaaren holds a BA from Harvard University, MA from the University of Cape Town, and JD from Columbia University. He is completing his PhD in the sociology of law at Yale University.

Toby Mendel is the Law/Asia Programmes Director with ARTICLE 19, Global Campaign for Free Expression, a leading international human rights NGO based in London. In that capacity, he has worked extensively on freedom of expression and freedom of information issues in Asia, Africa, Europe, the Middle East and Latin America. Mr. Mendel has published widely and been a frequent speaker at international conferences on a range of freedom of expression issues. Prior to joining ARTICLE 19, he worked for some time both in human rights and international development, including work as a senior human rights consultant with Oxfam Canada and a human rights policy analyst at the Canadian International Development Agency (CIDA). He has an honours BA in mathematics from McGill University and a first class LLB (law) from Dalhousie University, and is completing a PhD in international law at Cambridge University.

Kavita Modi completed her masters in Human Rights Law at University College in London in 2002. In 2002-2003, she worked at Liberty, one of the UK's leading human rights and civil liberties organizations, as the Director's researcher. She currently works in the Human Rights Department at Leigh, Day & Co. Solicitors.

Bimo Nugroho is Director of Institut Studi Arus Informasi (ISAI), the Institute for Studies on the Free Flow of Information, in Jakarta, Indonesia. The ISAI is a member of Indonesia's new Coalition for

Freedom of Information. Mr. Nugroho is co-author of "Indonesia's Underground Press," a study published in 2002 in the *International Journal for Communication Studies*. He was also a a participant in the 2001 International Roundtable on Journalism and Free Expression. He studied at the University of Indonesia.

Alasdair Roberts is an associate professor in the Maxwell School of Citizenship and Public Affairs at Syracuse University. He is also Director of the Campbell Public Affairs Institute at Syracuse University. A native of Pembroke, Ontario, Canada, Professor Roberts received a JD from the University of Toronto Faculty of Law in 1984, a Master's degree in Public Policy from the Kennedy School of Government at Harvard University in 1986, and a Ph.D. in Public Policy from Harvard University in 1994. He was a fellow at the Woodrow Wilson International Center for Scholars in Washington, DC in 1999-2000 and an Individual Program Fellow of the Open Society Institute in 2000-2001. His research focuses on two areas: public sector restructuring, and transparency in government. He received the Dimock Award for best lead article in *Public Administration Review* in 1995, and the Hodgetts Award for best English article in *Canadian Public Administration* in 2000.

John Wadham has been the Director of Liberty, one of the UK's leading human rights and civil liberties organisations, since 1995. He spent six years working for law centres in London and then in 1989 he qualified as a solicitor. He worked in private practice in a civil liberties firm for three years before moving to Liberty. In 1992 he was promoted to the post of Director of Law and Policy at Liberty and appointed Director in 1995. He has acted for a large numbers of applicants in cases before the Commission and Court of Human Rights. He is the co-editor of *Your Rights: The Liberty Guide*; the civil liberties section of the *Penguin Guide to the Law*; the caselaw reports for the *European Human Rights Law Review*; the co-author of *Blackstone's Guide to the Human Rights Act 1998* and *Blackstones Guide to the Freedom of Information Act 2000*. He is also editor of the Blackstones Human Rights Series. He was a member of the Government's Human Rights Act Task Force and has been commissioned to train many public authorities, senior officials, police officers, court staff and lawyers on the Human Rights Act and the European Convention on Human Rights.

NATIONAL SECURITY VS. OPENNESS:

AN OVERVIEW AND STATUS REPORT ON THE JOHANNESBURG PRINCIPLES

Toby Mendel
Law Programme Director
Article 19, Global Campaign for Free Expression

INTRODUCTION

The *Johannesburg Principles: National Security, Freedom of Expression and Access to Information,*[1] were adopted by a group of experts on October 1, 1995. Their goal was to set authoritative standards clarifying the legitimate scope of restrictions on freedom of expression on grounds of protecting national security. Since that time, the Principles have been widely endorsed and relied upon by judges, lawyers, civil society actors, academics, journalists and others, all in the name of freedom of expression. They set a high standard of respect for freedom of expression, confining claims based on national security to what States can legitimately justify.

Despite their status, most countries around the world are a very long way from having implemented the Principles. In most of the world, national security remains an excessively broad area of restriction, both in terms of punishing those who speak out and in terms of government secrecy. National security is also one of the most difficult areas for campaigners and human rights activists to promote reform, both politically and through the courts.

This is particularly true since September 11, 2001, as security logic dominates to the detriment of freedom of expression and as officials around the world arrogate to themselves even greater security powers. These powers are justified on the basis that they are needed to combat terrorism, but in practice they often lead to abuse of human rights. It does not help that some of the countries best-known for promoting and respecting human rights have also increased secrecy and rolled back rights in the aftermath of the terrorist attacks.[2]

Another unfortunate outcome of the attacks is that political energies are focused on combating terrorism rather than promoting human rights. Resources and attention are limited, and the overwhelming attention given to terrorism naturally undermines efforts in other areas. A related problem is that key international players have been willing to overlook human rights abuses as a trade-off for support in the fight against terrorism. A good example of this is Pakistan, where the international community had expressed serious concern about both the development of nuclear military capacity and the military takeover. These concerns were, however, summarily brushed aside in exchange for Pakistan's support for the war in Afghanistan.

Despite these problems, now is an appropriate time for human rights activists to consider how to address the issue of national security and to rekindle interest in the Johannesburg Principles and respect for the values they promote. Although security concerns remain very much at the forefront of global politics, there is an increasing scope to challenge the way in which these concerns undermine human rights. Furthermore, decision-makers are realising once again that, at root, security depends on promoting human rights. This is nowhere the case more than in the Middle East; the US, for example, is prioritising the promotion of freedom of expression and democracy in the Gulf countries.

This paper provides an overview of the main reasons why it has proven so difficult to ensure respect for freedom of expression in the face of national security concerns. It also provides an overview of the Johannesburg Principles, giving some examples of how they have, and have not, been implemented in practice. Finally, it points to some areas where more work is needed to assist campaigners in advocating for the implementation of the Johannesburg Principles.

NATIONAL SECURITY AND FREEDOM OF EXPRESSION

Freedom of expression is a fundamental, indeed foundational right, guaranteed under international law, all three main regional human rights treaties and almost every national constitution with a bill of rights.[3] Article 19 of the Universal *Declaration on Human Rights* (UDHR),[4] guarantees the right to freedom of expression in the following terms:

> Everyone has the right to freedom of opinion and expression; this right includes the right to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

The UDHR, as a UN General Assembly resolution, is not directly binding on States. However, parts of it, including Article 19, are widely regarded as having acquired legal force as customary international law since its adoption in 1948.[5] It is now increasingly accepted that this right includes the right to access information held by public authorities, commonly referred to as the right to freedom of information, or simply the right to information.[6]

Freedom of expression is a conceptually complex right because, although it is a fundamental, it is universally accepted that it may legitimately be subjected to restriction on various grounds. There is much debate at the national level about the test for restrictions, as well as the aims which such restrictions may legitimately serve but, at least under international law, the position is relatively clear, as set out in Article 19(3) of the *International Covenant on Civil and Political Rights* (ICCPR),[7] as follows:

> The exercise of the rights provided for in paragraph 2 of this article [the right to freedom of expression] carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> •For respect of the rights or reputations of others; and
>
> •For the protection of national security or of public order (*ordre public*), or of public health or morals.

This Article both stipulates clearly the aims which any legitimate restriction on freedom of expression must pursue – namely the rights or reputations of others, national security, public order, public health or public morals – as well as the test which any such restrictions must meet, namely that they are provided by law and are necessary.

Formally, this provision seeks to ensure that in imposing restrictions, States must balance the legitimate aim they seek to protect against the fundamental right to freedom of expression. In fact, however, apart from providing a procedural guarantee – that restrictions must be provided by law – it provides little guidance as to how any balancing is to take place. The aims listed are undefined and extremely broad, so that practically any legislation can arguably be accommodated and, in practice, international courts and tribunals rarely conclude that laws offend against freedom of expression on the basis that they do not pursue a legitimate aim.

The nub of the balancing takes place around the concept of necessity, a very context-dependent term. Unfortunately, international jurisprudence has done little to clarify the meaning of necessity. The European Court of Human Rights, for example, assessing a very similar phase in the *European Convention on Human Rights*,[8] has consistently interpreted the term necessity to mean:

> The Court must determine whether the interference at issue was "proportionate to the legitimate aim pursued" and whether the reasons adduced by the Austrian courts to justify it are "relevant and sufficient".[9]

This is a very subjective assessment, a fact to which the jurisprudence of the Court stands as testament. Some national courts have successfully elaborated far more precise tests.[10]

The conceptual problems with freedom of expression are perhaps at their highest in relation to considerations of national security. National security is a social value of the highest order, upon which the protection of all human rights, indeed our whole way of life, depends. It is universally accepted that certain restrictions on freedom of expression are warranted to protect national security interests. A State can hardly allow its citizens to divulge information about its troop movements during an active conflict, to give just one obvious example.

At the same time, historic abuse of restrictions on freedom of expression and information in the name of national security has been, and remains, one of the most serious obstacles with respect to freedom of expression around the world. These problems manifest themselves in two related but different areas. First, many States impose criminal restrictions on the making of statements which allegedly undermine national security. Cases based on these restrictions are relatively rare in democratic countries and are usually pretty high-profile and contentious, but they can be common in repressive countries where they may be used to suppress political opposition and critical reporting.[11] Second, in almost all States where freedom of information is guaranteed by law, these laws limit the right in relation to national security, often in very broad terms. Excessive secrecy in relation to national security is a widespread problem around the world, even in established democracies.[12]

Most of the traditional arguments in favour of openness apply with at least equal force where national security is concerned. Intelligence and security bodies play an important role in society and they must, like all public bodies, be subject to democratic accountability. In some cases, they appear not to be accountable even to elected officials. During and after the referendum process in East Timor, for example, the Indonesian authorities appeared to have little control over the armed forces and the militia who reported to them. In other cases, elected officials take advantage of the secrecy surrounding these bodies to abuse their powers for political purposes. Perhaps the most famous example of this is the abuses committed by Nixon which eventually led to his impeachment.

Defence industries absorb enormous amounts of public money and, in many countries, spend more, and more discretionary funds through contractual procedures than most if not all other public sectors. This is a natural breeding ground for corruption and it is only through open public oversight that this can be contained.

Public oversight is also crucial to ensure sensible policy- and decision-making, generally, but also specifically including in relation to national

security: "The problem with the 'national security state' is not so much that it violates … rights, although it sometimes does just that, but that it can lead to the repetition of irrational decisions."[13]

Malaysia – Political Abuse of National Security

Arrests under the Sedition Act, 1948, are commonly used for political purposes. For example, the popular online newspaper, malaysiakini, famous for its independent reporting, was raided by the Malaysian police on 20 January 2003 and 19 computers, including four servers, were seized for allegedly being in breach of the Sedition Act. Its crime was to publish a letter that satirised nationalist policies in favour of ethnic Malays by comparison to the United States, on the basis that this could cause racial disharmony.

In another recent example in October 2002, N. Gopalakrishnan, a senior member of the Parti Keadilan Nasional, an opposition party led by Wan Azizah, the wife of Anwar Ibrahim, was arrested for allegedly making serious allegations against the police force.

In some cases, the problem is simply repressive governments blatantly abusing their powers. But there are legitimate difficulties as well. What constitutes national security may be subject to very wide interpretation. In addition, the concept of necessity is particularly difficult in relation national security concerns and a lack of information, as well as the inability of non-experts, including judges to understand and assess threats to security, undermines oversight mechanisms.

One problem is that national security, unlike most areas of restricted freedom of expression, the very nature of the legitimate interest at stake is a highly political matter, involving an assessment of a threat, often from external sources. For example, faced with a restriction sought to be justified on the basis of privacy or public order, individuals have a broad, if subjective, social understanding against which to assess the potential for harm. The same is simply not true in relation to national security.

Compare, for example, a citizen's ability to independently assess claims that a demonstration would pose a public order risk and their ability to assess the risk posed to national security by Iraq.

This leads to a situation where security claims may be accepted, even though they are completely unwarranted. As Smolla has pointed out:

> History is replete with examples of government efforts to suppress speech on the grounds that emergency measures are necessary for survival that in retrospect appear panicky, disingenuous, or silly.[14]

This problem is compounded by the shroud of secrecy, sometimes legitimate, that surrounds national security matters. This means that courts, human rights organizations and others are asked to rely on circumstantial or tangential evidence. To continue the example above, very little of the evidence the U.S. and UK authorities' claim proves that Iraq has weapons of mass destruction has been make public, even to the UN Weapons Inspectors. The technical nature of many of the issues involved also makes it difficult for non-experts to accurately assess the risk.

These factors help to explain the high level of judicial deference, which sometimes seems absurd, in the face of national security claims. It is not only judges who face these problems; civil society actors also face a serious information and technical understanding gap. This acts as a brake on activism generally in this area and tends to perpetuate the culture of secrecy around national security.

Leander Case – Unwarranted Judicial Deference

Leander was dismissed from a job with the Swedish government on national security grounds, but was refused access to information about his private life, held in a secret police register, which provided the basis for his dismissal. He appealed to the European Court of Human Rights[15] claiming a breach of his rights to private life and freedom of expression. The Court found an interference with private life but held that this was justified as necessary to protect Sweden's national security.

Although no direct evidence was presented of the threat allegedly posed by Leander, the Court was prepared to accept that the official safeguards against abuse of the system were sufficient to satisfy the requirements of "necessity". It attached particular importance to the presence of parliamentarians on the National Police Board and to the supervision effected by various officials, including the Chancellor of Justice and the Parliamentary Ombudsman.

Ten years later, it transpired that Leander had been fired for his political beliefs and that the Swedish authorities had simply misled the Court. On 27 November 1997 the Swedish government officially recognized that there were never any grounds to label Leander a "security risk" and that he was wrongfully dismissed. They also paid him 400,000 Swedish crowns (approx. US$48,000) compensation.

THE JOHANNESBURG PRINCIPLES

Goals and Process

The primary goal of the Johannesburg Principles is to address the concerns noted above and, in particular, the lack of clarity under international law about the scope of legitimate restrictions on freedom of expression and information on national security grounds. High profile events – such as the so-called Spycatcher case in the UK,[16] the dismantling of apartheid in South Africa and the end of USSR and communism in Eastern Europe – all highlighted the need for reform in this area, as well as the need for clearer standards.

ARTICLE 19 and the Centre for Applied Legal Studies (CALS) at the University of Witswatersrand, South Africa, jointly convened a meeting of some 36 leading experts from every region of the world to discuss

this issue. On October 1, 1995, after intensive discussions and debate, the group adopted the Johannesburg Principles, setting out standards on the extent to which governments may legitimately withhold information from the public and prohibit expression for reasons of national security.

The idea was not to create new standards but to distill existing standards from a variety of sources of international and comparative law. As the Introduction states:

> 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.

The Principles aim to be at the cutting edge of international standards, playing a role in the positive development of these standards and reflecting the direction in which international law is, or should be, developed. At the same time, they have a solid legal basis, derived from the law and practice of democratic States, as well as in international standards. In other words, they seek to strike a balance between developing international and comparative standards and being rooted in this body of law.

The Principles have gained significant status since their adoption. Abid Hussain, the UN Special Rapporteur on Freedom of Opinion and Expression, in his 1996 annual report to the UN Commission on Human Rights, recommended that the Commission endorse the Principles.[17] They have been noted in the annual resolutions of the Commission on freedom of expression every year since 1996.[18] They have also been referred to by courts around the world,[19] and used by numerous decision-makers, NGOs, academics and others.

Overview of the Principles[20]

The Johannesburg Principles comprise 25 principles divided into four sections: General Principles, Restrictions on Freedom of Expression, Restrictions on Freedom of Information and Rule of Law and Other Matters. The section on General Principles reiterates the general guar-

antee of freedom of expression as it applies in the context of national security restrictions, defines national security and addresses emergencies and discrimination. The section on Rule of Law and Other Matters summarises general rights relating to due process and the right to a remedy, and addresses the issue of disproportionate punishments and prior censorship.

The main standard-setting principles are found in the sections on Restrictions on Freedom of Expression and on Restrictions on Freedom of Information. These sections set out the tests restrictions of expression and denial of access to information on the grounds of national security must meet. They also list various forms of expression that shall not be restricted on grounds on national security and provide for procedural protections for the right to information.

General Principles

Principle 1 reiterates the general guarantee of freedom of expression and the three-part test for restrictions on that right, with minor modifications to make them specifically relevant to the issue of national security. Principle 1.1 sets out the first part of the test, that restrictions must be prescribed by law, reiterating the standard requirements of such laws, namely that they be accessible, clear and narrowly drawn. It also adds the requirement that the law should provide for adequate safeguards against abuse, including judicial scrutiny. Although this is not normally associated with the guarantee of freedom of expression, it is inherent in the idea of an effective remedy for violations of rights, set out, for example in Article 2(3) of the ICCPR.

Principle 1.2, addressing requirement that restrictions on freedom of expression serve a legitimate aim, requires restrictions to have both the genuine purpose and the demonstrable effect of protecting national security. Thus either bad faith or ineffectualness will defeat a restriction.

Principle 1.3 elaborates on the concept of necessity in relation to national security, providing that any restriction must apply only where the expression poses a serious threat, it is the least restrictive means available and it is compatible with democratic principles. This is a higher standard than that applied by most international human rights courts and tribunals, both inasmuch as it sets a threshold barrier of serious harm and

that it requires the least restrictive means to be used. The threshold, however, is crucial since without it, States will be able to make national security-based claims for restrictions in excessively wide circumstances. The least restrictive means test is applied by a number of national courts[21] and has a solid principled basis. The European Court of Human Rights, however, has not applied this test, allowing States a 'margin of appreciation' when assessing rights, effectively a system of judicial deference to national authorities. However, the margin of appreciation doctrine has been widely criticised and the Court has limited its application in certain contexts.[22]

A narrow definition of a legitimate national security interest is provided in Principle 2, which draws its inspiration from The Siracusa Principles on the *Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*.[23] This provides that a restriction is not legitimate unless its purpose and 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" from either an internal or an external threat. This is probably an unrealistically high standard, despite its pedigree. The attacks of September 11, 2001, for example, could hardly be said to have threatened the existence or territorial integrity of the U.S., unless this is interpreted very broadly, which would largely defeat the purpose of a narrow definition.[24]

Principle 2 goes on to elaborate a number of illegitimate grounds for claiming a national security interest, such as protecting the government from embarrassment or entrenching a particular ideology. These are clearly not national security interests but, at the same time, countries around the world fail to respect this Principle.

Principle 3 deals with restrictions on freedom of expression pursuant to states of emergency. It repeats the conditions for imposing emergency rules under Article 4 of the ICCPR with a few differences. Principle 3 requires states of emergency to be in accordance with both national and international law and also explicitly imposes time limits on any emergency restrictions on freedom of expression. Most importantly, Principle 3, in contrast to Article 4, does not recognise the idea of derogations, limiting itself, instead, to the general concept of restrictions on freedom of expression. The guarantee of freedom of expression already explicitly recognises restrictions that are necessary, so this probably already implic-

itly covers emergency situations. Indeed, it is arguable that the emergency standard – "strictly required" - may not represent a higher standard that the default necessity one, in effect rendering the emergency power to apply restrictions superfluous.

Egypt, Syria – States of Emergency

The rules on states of emergency are flouted in many countries. Egypt, for example, has had a state of emergency in place more-or-less continuously since it was first imposed in 1958 and Syria has had an emergency law in place since 1962.

The Egyptian emergency law confers wide-ranging and arbitrary powers on the president to censor the print media prior to publication and to confiscate or close down their printing facilities in the interests of "public safety" or "national security." Trials held under the emergency law are heard by special State Security Courts and their verdict is not subject to appeal. The law has been used to detain thousands of people suspected of opposing the government. Threats to public safety and security have been interpreted very widely to include the actions of suspected supporters and sympathisers of unarmed Islamist groups. In a celebrated case, the sociology professor, Saad Eddin Ibrahim, was sentenced to seven years in prison in 2001 by a State Security Court for contravening a military order issued in 1992 pursuant to powers under the emergency law. The conviction was later overturned.

A prohibition on discrimination when restricting freedom of expression is provided for in Principle 4, which closely parallels Article 26 of the ICCPR, prohibiting any discrimination by law on a number of grounds. Given that the guarantee of freedom of expression only permits restrictions provided by law, these necessarily fall within the ambit of Article 26.

Restrictions on Freedom of Expression

The international guarantee of freedom of expression provides for an

unqualified right to hold opinions without interference and this is reflected in Principle 5.

The key test for restrictions on freedom of expression in the name of national security is set out in Principle 6, which subject to other principles, prohibits restrictions on expression unless:

- the expression is intended to incite imminent violence;
- it is likely to incite such violence; and
- there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.

At the root of this principle are two central ideas. First, there is a difference between beliefs and actions and, in turn, between inciting to beliefs and inciting to actions. It may be noted that this rule applies only in the context of national security.[25]

The potential for abuse of a rule prohibiting incitement to beliefs is fairly obvious. Whereas actions are clear, there are serious definitional problems with the idea of illegal beliefs. It is not possible, for example, to maintain a principled difference between an academic theory about the use of violence and a party articulating its belief in such violence. Furthermore, political rhetoric can take extreme forms and a rule prohibiting incitement to beliefs could be used to silence opposition parties or critics. Perhaps most importantly, however, there is simply no basis for arguing that beliefs pose a sufficient threat to security to warrant overriding a fundamental right. A simple belief that violence or unlawful activities are necessary to change society, of itself, does little or no tangible harm.

Second, this Principle reflects the idea that there must be a very close nexus between the expression and the risk of violence. Courts around the world have stressed this when assessing the legitimacy of restrictions on freedom of expression. Due to the very general nature of national security, a wide range of harmless speech could be banned in the absence of a requirement of a close nexus between the speech and the risk of harm. The Turkish authorities, for example, have banned Kurdish poems on the grounds that they promote nationalism and threaten territorial integrity.[26] The box below sets out some of the statements on this issue made by national courts. Despite these positive

statements, most countries, as well as international courts, still have a very long way to go in recognising and respecting this standard.[27]

National Courts and Incitement to Violence

The following are a few statements made by national courts in assessing the required nexus between expression and a risk of harm to national security or the closely related problem of public order.

India:

> The anticipated danger should not be remote, conjectural or far fetched. It should have proximate and direct nexus with the expression. The expression should be intrinsically dangerous…. In other words, the expression should be inseparably locked up with the action contemplated like the equivalent of a 'spark in a powder keg'.[28]

United States:

> [T]he constitutional guarantees of free speech and free press do not permit a state to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.[29]

South Africa:

In *S. v. Nathie*, the appellant was charged with inciting offences against the Group Areas Act in the context of protests against the removal of Indians from certain areas. The appellant stated, inter alia: "I want to declare that to remain silent in the face of persecution is an act of supreme cowardice. Basic laws of human behaviour require us to stand and fight against injustice and inhumanity." The Court rejected the State's claim of incitement to crime, holding that since the passage in question did not contain "any unequivocal direction to the listeners to refuse to obey removal orders" it did not contravene the law.[30]

Principles 7-9 set out a number of specific examples of expression that shall not be considered a threat to national security. These are, by-and-large, uncontroversial, including things such as advocating change of government policy, criticizing the State or government, objecting to military service, transmitting information about a banned organisation,31 or using minority languages. As with the second part of Principle 2, however, all of these restrictions have been applied in the past, purportedly to protect national security, and many countries continue to apply them.

UK – Banning Reporting on 'Terrorist' Groups

The British Broadcasting Act grants the power to the authorities to prohibit broadcasting of certain material, a power which in terms of the Act would appear to be unlimited. In October 1988, the then Home Secretary, Douglas Hurd, issued notices banning any matter which included words spoken by persons representing a list of banned organisations, including Sinn Féin, a legal political party. The ban was appealed to the European Commission on Human Rights, which rejected the complaint as manifestly unfounded, in effect holding that the ban clearly fell within the scope of legitimate restrictions on freedom of expression.[32]

The BBC and other British broadcasters effectively made a mockery of the rule by using Irish-accented voiceovers when presenting statements from the banned organisations. This is another example of the excessive defence of courts to security claims.

Principle 10 provides that States have an obligation to prevent private groups from interfering with freedom of expression. This is consistent with international case law, particularly from the Inter-American Court of Human Rights[33] but now also affirmed by the European Court of Human Rights.[34] There is little national case-law on this, in part because the problem does not arise in those countries where courts might accept these principles. The growing body of international case law, however, is very much the tip of the iceberg, and in many countries there is, instead of protection, collusion between the authorities and the 'private' actors perpetrating the abuse.

The right to access information held by public authorities has now gained widespread recognition but its status was far less established in 1995, when the Johannesburg Principles were drafted. Despite this, Principle 11 clearly recognises this right, as an aspect of the right to freedom of expression, subject to restriction only in accordance with the three-part test for all restrictions on freedom of expression. This right is now accepted in all regions of the world, as evidenced by the rapid growth in the number of countries that have passed freedom of information legislation – with the possible exception of Africa, where to date only South Africa and Zimbabwe35 have passed such a law – as well as in a number of authoritative international standards. However, the extent to which such legislation respects the three-part test for restrictions, as well as a number of other established principles, varies considerably.

Since the adoption of the Johannesburg Principles, there have been a number of significant developments regarding freedom of information, which applies to all information held by public authorities, not just information relating to national security. ARTICLE 19 has encapsulated these developments in two standard-setting documents, *The Public's Right to Know: Principles on Freedom of Expression Legislation*[36] and *A Model Freedom of Information Law*.[37] These set out in far more detail general standards and processes relating to freedom of information. Principle 4 of *The Public's Right to Know*, in particular, sets out a three-part test for exceptions to the right to access information, based on but slightly different from the general test for restrictions on freedom of expression, as follows:

- the information must relate to a legitimate aim listed in the law;
- disclosure must threaten to cause substantial harm to that aim; and
- the harm to the aim must be greater than the public interest in having the information.

Principle 12 provides that States 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." This is consistent with the "prescribed by law" part of the test for restrictions, and in particular that restrictions should be clear and narrowly drawn. Despite this, most laws simply list 'national security' as a ground for restricting access to information without defining this term at all, let

Recognition of the Right to Freedom of Information

Freedom of information has been recognised as an aspect of the right to freedom of expression by UN officials, as well as all three regional human rights systems. In November 1999, the three special mandates on freedom of expression – the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression – meeting together for the first time under the auspices of ARTICLE 19, adopted a Joint Declaration which included the following statement:

> Implicit in freedom of expression is the public's right to open access to information and to know what governments are doing on their behalf, without which truth would languish and people's participation in government would remain fragmented.[38]

Declarations or Recommendations adopted by the Committee of Ministers of the Council of Europe, the African Commission on Human and Peoples' Rights and the Inter-American Commission on Human Rights have all affirmed the right to access information held by public officials.[39]

These official statements have been accompanied by a significant trends towards the adoption of freedom of information legislation all over the world during the last decade with laws having been adopted in the last five years in all regions of the world including Europe (e.g. Bosnia- Herzegovina, Romania and Slovakia), Africa (e.g. South Africa and Zimbabwe), Latin America (e.g. Mexico and Peru) and Asia (e.g. Japan, Thailand and India).

alone providing a specific list of categories of exceptions. In many cases, these laws do not even require the disclosure to pose a risk of harm to national security. Even where they do, as the box below illustrates, countries have found ways to limit disclosures.

Even when the disclosure of information is likely to harm a legitimate interest, it should still be subject to disclosure unless the harm outweighs the public interest in accessing the information. This is a logical inference from the principles underlying freedom of information and is reflected in many laws. A public interest override of this sort is necessary since it is not possible to frame exceptions sufficiently narrowly to cover only information which may legitimately be withheld. Furthermore, a range of circumstances, for example the presence of corruption, will generate an overriding public interest in disclosure. Principle 13 reflects this, providing that in decisions on information disclosure, the public interest "shall be a primary consideration". Principle 13 differs slightly from the last element of the three-part test in Principle 4 of The Public's Right to Know, set out above. In particular, the latter requires the harm to the protected interest to outweigh the public interest in disclosure, a more stringent, or at least more clearly stringent, standard.

New Zealand, UK – Broad National Security Exceptions

The New Zealand Official Information Act, 1982 contains an exception for material likely to prejudice the security or defence of New Zealand. Although this does incorporate a harm test, the law also provides that a ministerial certificate shall be conclusive evidence of the threat, effectively granting the minister unsupervised power to classify information (see sections 6 and 7). The UK Freedom of Information Act, 2001, exempts information where this is "required for the purpose of safeguarding national security" but also provides for a ministerial override (section 24).

Principle 14 requires States to put in place "appropriate measures to give effect to the right to obtain information", including a right of

review by an independent authority and finally by the courts. Experience in many countries with constitutional guarantees for freedom of information but no legislation to implement these guarantees bears testament to this need. The Public's Right to Know makes it clear that specific implementing legislation is required to give effect to freedom of information and sets out in some detail the procedural and appeal mechanisms which such legislation should provide for.

The NATO Conundrum

Most countries in East and Central Europe have recently passed freedom of information laws and some of these laws provide a very solid basis for government openness. However, many of these countries also want to join NATO which, as a security organisation, requires certain minimum standards of secrecy. As a result, countries such as Romania and Bulgaria have followed up their freedom of information laws by passing secrecy or classification laws which seriously undermine the earlier openness legislation. Unfortunately, the NATO secrecy standards are themselves set out in a classified document, C-M(2002)49. This document has remained secret notwithstanding the clear illegitimacy of withholding a classification standards document, and despite the best efforts of a group of people trying to access it both directly from NATO and via national freedom of information laws.

Principle 15 prohibits punishment for disclosure of information if this does not result in actual harm, or a likelihood thereof, or where the overall public interest is served by disclosure. This applies, for example, to situations where the media discloses classified information but it also covers civil servants applying, as it does, to everyone. This Principle recognises that no matter how well freedom of information legislation is designed, there will still be cases where disclosure is refused and it is only through a leak that important information, for example exposing corruption or wrongdoing, may become public. Indeed, the unauthorised release of classified information serves as an important safety value for ensuring the flow of information to the public, a social role which is recognised in the law and practice of a number of countries.40

In fact, the principle is not as controvrsial as it may seem since, in the absence of a showing of harm, or where this is in the overall public interest, information should anyway be subject to disclosure.

The relationship between Principles 6 and 15 is not entirely clear. Although formally Principle 6 applies subject to Principle 15, they overlap considerably. Principle 6 applies to all expression while Principle 15 covers "disclosure of information." All disclosure of information is expression (so Principle 15 falls entirely within the scope of Principle 6) and most expression, apart perhaps from pure opinions, involves some disclosure of information. It might be preferable to interpret Principle 15 as being restricted in scope to confidential information, given that it imposes a much lower standard on restrictions than Principle 6.

Malawi – Constitutional Guarantee without Implementing Legislation

Article 37 of the Malawian Constitution contains the following guarantee of freedom of information:

> Subject to any Act of Parliament, every person shall have the right of access to all information held by the State or any of its organs at any level of Government in so far as such information is required for the exercise of his rights.

The lack of implementing legislation has seriously undermined respect for this right in practice, despite its limited nature, applying as it does only to information needed to exercise a right.

Principle 15 should probably also be restricted in scope to civil servants and public officials. In the UK, for example, the Official Secrets Act, 1989, prohibits secondary disclosure of classified information, for example by journalists, under more stringent conditions than those set out in Principle 15 and yet this rule has been widely criticised by the media and free speech advocates. It will always be controversial to punish secondary disclosures, so prosecutions are rare in democratic countries. It is the responsibility of the government to ensure that

secret information is adequately protected and not of journalists to assess when and whether disclosure will cause harm. Indeed, there are serious problems with imposing a burden of this sort on private actors, at least where the criminal law is concerned.

Principle 16 applies specifically to civil servants and protects them against any detriment, including employment-related sanctions, for disclosure of information learned by virtue of government service, where this is in the overall public interest. This is again consistent with the test for exceptions to freedom of information, which, if applied, should mean that this information is, at least upon request, subject to mandatory disclosure. A Model Freedom of Information Law has added a refinement to this rule, providing that individuals who disclose information on wrongdoing or harm, commonly known as whistleblowers, should be protected against sanction, "as long as they acted in good faith and in the reasonable belief that the information was substantially true and disclosed evidence of wrongdoing or a serious threat

UK – David Shayler Case

The high-profile case of David Shayler in the UK illustrates the need for whistleblower protection. Shayler, a former MI5 Intelligence Officer, was charged, and ultimately convicted, under section 1(1) of the Official Secrets Act, 1989 for various allegations, including that MI5 had plotted to assassinate the Libyan leader, Colonel Gaddafi. It is clearly a matter of great public interest that any serious allegation of this nature be subject to independent investigation.

Neither a public interest defence nor a defence based on the fact that the disclosure had not actually harmed security was available to Shayler, who was ultimately convicted. The House of Lords held that these defences were not necessary because Shayler could have used internal complaints procedures or gone to his superiors, and that ultimately he could have sought judicial review of his superiors' decision. This seems to woefully underestimate the practical difficulties associated with these courses of action.

to health, safety or the environment."[41] Relative to the standard in Principle 16, this relieves them from having to assess whether the disclosure is in the public interest, something they are not qualified to do. A number of countries have adopted specific legislation to protect whistleblowers.

Subsequent ARTICLE 19 standard-setting has also added protection for individuals who disclose information pursuant to freedom of information legislation, as long as they acted reasonably and in good faith, even if they make mistakes.[42] This is important to help address the culture of secrecy in government and to give civil servants the confidence to disclose information under freedom of information legislation.

South Africa – Whistleblower Protection

The South African Protected Disclosures Act, 2000, provides protection against employment-related sanctions for disclosures which reveal various types of wrongdoing or risks of harm, including criminal activities, the failure to comply with a legal obligation, a miscarriage of justice, health or safety risks, harm to the environment or discrimination. Disclosures are protected if they are made to legal practitioners, via formal employment complaints procedures or to various high-level officials, such as ministers. Disclosures are also generally protected, including for example to the media, where they are made in good faith and in the reasonable belief that they are true and where one of the following conditions is met:

- the employee has reason to believe he or she will be sanctioned for making the disclosure;
- there is no complaints procedure and the employee has reason to believe the wrongdoing or harm will be concealed;
- a similar disclosure has already been made to no effect; or
- the risk is of exceptionally serious wrongdoing or harm.

Principle 17 provides that it is not legitimate to try to prevent further publication of a document which is already public which, although obviously logical, has sought to be denied in a number of countries.[43] The growing prevalence of the Internet will soon render nugatory any efforts by the authorities in most countries[44] to prevent further publication. Indeed, the Internet community will almost invariably undercut attempts to prevent further publication by mirroring websites and by widely publicising target documents.

The right of journalists to protect the secrecy of confidential sources of information is recognised in Principle 18, which prohibits orders of source disclosure based on national security interests. International law recognises this right, although not in absolute terms. The European Court of Human Rights, for example, has stated that restrictions to this right must be, "justified by an overriding requirement in the public interest."[45] A serious national security risk would presumably meet this test. A number of countries around the world, however, protect source confidentiality even in light of a national security claim while others place severe restrictions on source disclosure in this context.[46]

Control over Information During Conflict

An interesting example of manipulation of information during an ongoing conflict relates to the failed US raid of 19 October 2001 on Afghan territory, which was successfully repulsed by Taliban forces. The Taliban reported significant numbers of US fatalities, whereas in fact no Americans were killed. The US authorities, on the other hand, claimed the next day that the raid had been a success, with General Richard Myers, Chairman of the US Joint Chiefs of Staff, stating that it had been conducted "without significant interference from Taliban forces". The US authorities even released footage demonstrating this, later revealed to be showcased rather than actual, acknowledging only much later that the raid had led to a number of casualties.

Principle 19 addresses the issue of access to restricted areas, ruling out restrictions that "thwart the purposes of human rights and humanitarian

law". It also provides that States may limit access to zones of conflict only where this is necessary to protect the safety of others. This rule has probably not been observed in practice since the Vietnam war and security forces certainly do not facilitate access. Indeed, in most modern conflicts, the authorities have sought as far as possible to maintain control over, and indeed manipulate, information.

Rule of Law and Other Matters

Principles 20, 21 and 22 deal with various due process and rule of law issues, including pre-trial and trial rights, the right to all available remedies and the right to trial by an independent, civilian court. These provisions are based on, and in some cases elaborate further, rights protected by the ICCPR.

Sri Lanka – Prior Censorship

On 3 May 2000, the President of Sri Lanka adopted emergency regulations that provided for the appointment of a censor with the power to require newspapers to submit in advance material on certain subjects. The censor issued a directive requiring any material relating to national security to be vetted by his office. The Sunday Leader, a local English-language daily was held in breach of this rule three times: for publishing a photo of an opposition rally, for publishing two almost identical cartoons, one targeting the opposition, which had not been censored, and one targeting the governing party, which had been completely censored (so publication was in breach of the rules), and for publishing a spoof entitled "War in Fantasy Land – Palaly is not under attack". The censor then banned the newspaper, which appealed this to the Supreme Court on constitutional and procedural grounds. The Court struck down the censorship regime, and the ban on The Sunday Leader, ostensibly on the basis that the censor had not been appointed properly. However, the ruling effectively brought the system of prior censorship to an end.

Principle 23 prohibits prior censorship to protect national security except in case of an emergency which meets the conditions of Principle 3. Prior censorship is not defined but it can be understood in two ways, either as a system for vetting certain means of communication, such as books or films, before they are made public (for example, by an official censor) or as any measure which prevents or delays original dissemination to the public (this would include, for example, a court injunction). The Johannesburg Principles use this term in its latter, broader sense.

US – Prior Restraint

The US Supreme Court has all but ruled our prior restraints and has never upheld one on national security grounds. In particular, the Court has set out the following conditions on any prior restraint:

- the material would pose a threat of immediate and irreparable harm to a "near sacred right";
- the measures would be effective; and
- no other less restrictive measures would be effective.[50]

This Principle thus limits prior censorship measures to situations where there is a legitimate emergency in place and where the measures are "strictly required by the exigencies of the situation". As has already been noted, this standard may not actually be any more stringent than the requirement of necessity that applies to all expression. The European Court of Human Rights has been relatively conservative about prior restraint, but has at least held that it calls, "for the most careful scrutiny on the part of the Court."[47] The American Convention of Human Rights, however, rules out any form of prior censorship except to protect children and adolescents.[48] The prohibition on prior censorship has been upheld by the Inter-American Court of Human Rights in a case finding a breach in relation to the banning of a film.[49]

Principle 24 rules out punishments for expression which are disproportionate to the seriousness of the offence. It is now clear that international guarantees of freedom of expression not only set standards relating to

restrictions themselves, but also the sanctions which may result from breach of a restriction.[51]

Finally, Principle 25 provides that the Principles shall not be interpreted as restricting established human rights.

FUTURE WORK

The Johannesburg Principles have made a considerable contribution to clarifying the appropriate standards for national security-based restrictions on freedom of expression. However, they fail to provide specific guidance on one key issue: what information, in practice, is it legitimate to withhold on grounds of national security. Principle 12 requires States to designate specific and narrow categories of information that may be withheld, but the Principles provide no guidance as to what these categories might look like beyond the general test for restrictions on freedom of expression.

A concrete example, much debated, is whether and to what extent defence expenditures must be made public. It if fairly obvious that some detail is required if effective public oversight is to prevent corruption and mismanagement in relation to military procurement. On the other hand, States claim a right to some secrecy here, so as not to undermine their capacity to respond to an attack by exposing their potential to the enemy. Obviously this question can never be answered in the abstract, but guiding principles could at least set limits on the scope of secrecy claims.

A closely related issue, noted above, is that Principle 2, defining a legitimate national security interest, is not sufficiently clear. A more precise definition of national security, reflecting the actual practice of those States which are least restrictive in this area, would provide a better underpinning for the Principles and also help answer the question posed above.

There is clearly no question of revising or reissuing the Johannesburg Principles themselves, and this is in no way necessary or desirable. Rather, supplementary material needs to reinforce them. A starting point may be research on the practice in these areas by the more open democracies around the world. This could lead to the formulation of guidelines as to legitimate categories of secrecy, as well as the scope of those categories.

NOTES

[1] ARTICLE 19 (London: 1996).

[2] In Canada, for example, the *Anti-Terrorism Act*, S.C. 2001, c. 41, gave the Attorney General the power to issue certain confidentiality certificates which excludes the related records from the operation of the Access to Information Act and discontinues any related investigation by the commissioner or any court.

[3] As well as some that do not include such bills. See, for example, *Australian Capital Television v. The Commonwealth; State of New South Wales v. The Commonwealth* (1992) 177 CLR 106 (High Court of Australia), holding that the right to freedom of political communication was implicit in the structure of elected government provided for by the constitution.

[4] UN General Assembly Resolution 217A(III), 10 December 1948.

[5] See, for example, *Filartiga v. Pena-Irala*, 630 F. 2d 876 (1980) (US Circuit Court of Appeals, 2nd Circuit).

[6] See below, under Restrictions on Freedom of Information.

[7] UN General Assembly Resolution 2200A(XXI), adopted 16 December 1966, in force 23 March 1976. The ICCPR is an international treaty ratified by some 149 States as of December 2002.

[8] Adopted 4 November 1950, in force 3 September 1953.

[9] *Lingens v. Austria*, 8 June 1986, Application No. 9815/82, para. 40.

[10] See, for example, *R. v. Oakes* [1986] 1 SCR 103 (Supreme Court of Canada), p. 138-9. The so-called 'Oakes' test requires courts to ask three questions: are the measures adopted carefully designed to achieve the objective in question (the rational connection question); do the means impair the right or freedom in question as little as possible; and are effects of the measures proportionate to the objective.

[11] See box below on Malaysia.

[12] See the box below on the David Shayler case from the UK.

[13] Chevigny, Paul, "Information, the Executive and the Politics of Information" in Shetreet, Simon, ed., *Free Speech and National Security* (Dordrecht: Martinus Nijhoff, 1990).

[14] Smolla, Rodney, *Free Speech in an Open Society* (New York: Knopf, 1992), p. 319.

[15] *Leander v. Sweden*, 26 March 1987, Application No. 9248/81.

[16] *The Observer and Guardian v. United Kingdom*, (Spycatcher case), 26 November 1991, Application No. 13585/88, 14 EHRR 153, para. 60 (European Court of Human Rights).

[17] Report of the Special Rapporteur, *Promotion and protection of the right to freedom of opinion and expression*, UN Doc. E/CN.4/1996/39, 22 March 1996, para. 154.

[18] See, for example, Commission Res. 1996/53, preamble.

[19] See, for example, *Gamini Athukoral "Sirikotha" and Ors v. Attorney-General*, 5 May 1997, S.D. Nos. 1-15/97 (Supreme Court of Sri Lanka) and *Secretary of State for the Home Department v. Rehman* [2001] UKHL 47 (House of Lords).

[20] This part of the paper draws on Coliver, Sandra, "Commentary on the Johannesburg Principles on National Security, Freedom of Expression and Access to Information" in Coliver, S., Hoffman, P., Fitzpatrick, J. and Bowen, S., eds., *Secrecy and Liberty: National Security, Freedom of Expression and Access to Information* (Dordrecht: Martinus Nijhoff, 1999).

[21] See, for example, note 10 and Coliver, note 20, pp. 30-31.

[22] See, for example, *Goodwin v. the United Kingdom*, 27 March 1996, Application No. 17488/90, 22 EHRR 123.

[23] UN Doc. E/CN.4/1985/4, Annex, on-line at http://www.article19.org/docimages/1500.doc and reprinted in (1985) 7 *Human Rights Quarterly* 3.

[24] Coliver, note 20, p. 19, states: "[I]t is not necessary that public disturbances threaten to erupt throughout the country, but their effects must be felt throughout". This is not substantiated by the text and, in any case, introduces an unacceptably subjective, broad concept to the otherwise clear definition.

[25] It would not, for example, apply to a law prohibiting incitement to hatred which was aimed at preventing discrimination.

[26] See, for example, *Karatas v. Turkey*, 8 July 1999, Application No. 23168/94 (European Court of Human Rights).

[27] Coliver, note 20, p. 38, states bluntly: "Principle 6 is not yet an accepted norm of international law."

[28] *S. Rangarajan v. P.J. Ram* [1989](2) SCR 204, p. 226 (Indian Supreme Court).

[29] 395 U.S. 444, 447 (1969) (US Supreme Court).

[30] [1964](3) SA 588 (A), p. 595 A-D.

[31] But see the box below, on the UK.

[32] *Brind & Ors v. United Kingdom*, 9 May 1994, Application No. 18714/91.

[33] See, for example, *Velásquez Rodríguez v. Honduras*, 29 July 1988, Series C, No. 4.

[34] *Gundem v. Turkey*, 16 March 2000, Application No. 23144/93 .

[35] The Zimbabwean Access to Information and Protection of Privacy Act does formally provide for a right to freedom of information but this is largely undermined by exceptions and most of the Act is about controlling journalists and the media.

[36] ARTICLE 19: London, 1999. Available on the ARTICLE 19 website at: http://www.article19.org/docimages/512.htm.

[37] ARTICLE 19: London, 2001. Available on the ARTICLE 19 website at: http://www.article19.org/docimages/1112.htm. Both documents are also available via the ARTICLE 19 online Handbook, http://handbook.article19.org, under Key Documents.

[38] 26 November 1999. See also, Report of the UN Special Rapporteur, Promotion and protection of the right to freedom of opinion and expression, UN Doc. E/CN.4/2000/63, 18 January 2000, paras. 42-44

[39] Recommendation R(2002)2 the Committee of Ministers of the Council of Europe on access to official documents, adopted on 21 February 2002; the Declaration of Principles on Freedom of Expression in Africa, adopted by the African Commission on Human and Peoples' Rights at its 32nd Session in October 2002; and the Inter-American Declaration of Principles on Freedom of Expression, adopted by the Inter-American Commission Human Rights on 19 October 2000 at its 108th Regular Session.

[40] See Coliver, note 20, pp. 63-65.

[41] Note 37, section 47.

[42] Ibid., section 48.

[43] See, for example, *The Observer and Guardian v. United Kingdom*, (Spycatcher case), 26 November 1991, Application No. 13585/88, 14 EHRR 153, (European Court of Human Rights).

[44] Most NGOs, academics and other civil society actors now have access to the Internet and broad public access is growing rapidly in most parts of the world.

[45] *Goodwin v. the United Kingdom*, 27 March 1996, Application No.

17488/90, 22 EHRR 123, para 39.

[46] See Coliver, note 20, pp. 69-70.

[47] *The Observer and Guardian v. United Kingdom*, (Spycatcher case), 26 November 1991, 14 EHRR 153, para. 60.

[48] Adopted 22 November 1969, O.A.S. Treaty Series No. 36, 1144 U.N.T.S. 123, in force 18 July 1978, Article 13.

[49] "The Last Temptation of Christ" case (*Olmedo Bustos et al. vs. Chile*), 5 February 2001, Series C, No. 73, para. 72.

[50] See Coliver, note 20, p. 78.

[51] See, for example, *Tolstoy Miloslavsky v. United Kingdom*, 13 July 1995, Application No. 18139/91 (European Court of Human Rights).

NATIONAL SECURITY AND OPEN GOVERNMENT IN THE UNITED STATES:

BEYOND THE BALANCING TEST

Thomas S. Blanton
Director, National Security Archive
George Washington University

INTRODUCTION

National security is not a value in itself, but rather a condition that allows a nation to maintain its values.[1] In contrast, open government is both a condition and a value of democratic societies. Thus, putting the two concepts on the same spectrum, or speaking of them as in some kind of balance with each other, gives excessive weight to the former, and diminishes the necessary suspicion that should greet any attempt to reduce openness on national security grounds. We need a new paradigm beyond the balancing test, else security concerns of the day will continue to erode fundamental values.

Such erosion is not new in the United States, since secrecy attended the birth of this country at the Constitutional Convention of 1787. But the government's enormous information security and classification system is a more recent phenomenon, an aging child of the Cold War that not only refuses to go quietly into retirement, but finds a fountain of youth in wars of all kinds.

The new secrecy trend actually began before the Bush administration,

during the partisan battles of the late Clinton years. In turn, the Bush administration's retrenchment began before 9/11, but the shock of 9/11 provided the government with political capital and U.S. public support for greater secrecy in the name of national security. The current information war features battles on many fronts: scientific and technical information, presidential records, implementation of the Freedom of Information Act, on-line censorship, public safety information, and more. The bottom line is that the new secrecy is not as bad as it could be, but much worse than it should be.

At the same time, a new paradigm is beginning to emerge – partly based on the scientific critique of secrecy, but even more so on the secrecy failures surrounding 9/11 – that posits instead of a balancing act, an extreme limitation on secrecy and an emphasis on openness as the most important guarantor of security.

The following provides a highly selective historical background for U.S. limitations on openness in the name of national security, a brief and idiosyncratic description of how the Cold War created the modern national security secrecy system, a revisionist review of the roots of U.S. retrenchment in the late 1990s, a theological discussion of the origins of Bush administration secrecy, a succinct tour guide's map of the main battlefronts in the current information wars, and finally, more of a wishlist than a prognosis for the new paradigm that is emerging in large part from the ashes of the World Trade Center.

HISTORICAL BACKGROUND

From earliest days of the American republic, born as it was in revolution (which is to say, treason against Great Britain), national security secrecy was a fundamental feature of governance. The coordination of the revolution itself rested in the hands of two committees created by the Continental Congress, one a "Secret Committee" that handled weapons purchases and war materials, and the second a "Committee of Secret Correspondence" that handled foreign relations. The Constitutional Convention of 1787, after the revolution, met in closed sessions (the proceedings were not published until 1819); and James Madison – the author of the famous quotation about "a people who

mean to be their own Governors, must arm themselves with the power which Knowledge gives" – justified the convention's secrecy on the grounds that delegates had to be protected from outside pressures until consensus could form (which took 30 years).[2]

The U.S. Constitution itself contains only one specific mention of secrecy, in Article I, Section 5, which states:

> Each House shall keep a Journal of its Proceedings, and from time to time publish the same, excepting such Parts as may in their Judgment require Secrecy; and the Yeas and Nays of the Members of either House on any question shall, at the Desire of one fifth of those Present, be entered on the Journal.

This original Constitutional mandate does not posit a balancing test for secrecy, or even a "tension" between openness and secrecy.[3] Instead, the Constitution compels publicity for the Congress's proceedings and accountability for its actions, with secrecy as the exception that proves the rule.

Congress's public functioning largely conceded the secrecy field to the Article II powers vested in the President as commander-in-chief and as maker of treaties (with the advice and consent of the Senate), where we can see early intimations of the massive secrecy system of today. In the first U.S. administration, President George Washington imposed secrecy on provisions of various treaties with Native American tribes, and in 1796 he denied Congress access to secret negotiation documents, writing:

> The nature of foreign negotiations requires caution, and their success must often depend on secrecy; and even when brought to a conclusion a full disclosure of all the measures, demands, or eventual concessions which may have been proposed or contemplated would be extremely impolitic; for this might have a pernicious influence on future negotiations, or produce immediate inconveniences, perhaps danger and mischief, in relation to other powers. The necessity of such caution and secrecy was one cogent reason for vesting the power of making treaties in the President, with the advice and consent of the Senate, the principle on which that body was formed confining it to a small number of

members. To admit, then, a right in the House of Representatives to demand and to have as a matter of course all the papers respecting a negotiation with a foreign power would be to establish a dangerous precedent.[4]

Subsequently, in 1798, the U.S. government arrested the editor of the *Philadelphia Aurora* (who was Benjamin Franklin's grandson) on common law charges of seditious libel against the President, for printing the text of a treaty under secret consideration by the Senate. (But an 1812 Supreme Court decision overturned the notion of common law seditious libel, and it was not until World War I that significant new prosecutions on these grounds arose.)[5]

The very first appropriation by the U.S. Congress gave President Washington a secret account for spying. On July 1, 1790, Congress approved a $40,000 "Contingent Fund of Foreign Intercourse" that allowed the President to spend the money by voucher without indicating either the purpose or the person to whom the money was paid. Within three years, this fund had grown to $1 million, or about 12 percent of the national budget, and was used primarily to ransom American citizens from the Barbary pirates and to bribe foreign officials.[6] This was something of an exception to the general principle, so strongly enunciated by Madison and others, that to allow the combination of the "power of the purse" with the "power of the sword" was to descend into dictatorship. (This fund provided precedent for the CIA's "unvouchered" funds beginning in 1947, with acquiescence from Congress.) Perhaps the most important turning point in this early history of national security and openness was Washington's decision to step down after two terms as President, rather than continuing as Commander-in-Chief-for-life.[7] His successors enjoyed lesser and varying degrees of standing to enforce secrecy claims, and the relatively small size of the federal government and its associated militia and diplomatic corps meant that secrecy processes remained both limited and ad hoc. No additional secret funds were created until the 20th century, and the one extant example of secret legislation, the No-Transfer Act of 1811 – which empowered the President to seize any part of Florida if any foreign power attempted to occupy the area – was published seven years later, in 1818.[8]

Even during the Civil War of the 1860s, there was no formal or official system of military secrecy. President Lincoln famously wrote to one of his commanders, who sought to censor local press coverage, that

> [y]ou will only arrest individuals and suppress assemblies or newspapers when they may be working palpable injury to the military in your charge, and in no other case will you interfere with the expression of opinion in any form or allow it to be interfered with violently by others. In this you have a direction to exercise great caution, calmness, and forbearance.

In general, despite Lincoln's suspension of habeas corpus and examples of suppression of newspapers, most war-related information was readily available to the public.[9]

Typical of the rather limited application of national security secrecy in the pre-Cold War era was the first formal secrecy procedure, in the Army General Order of 1869, which covered only the physical layout of forts. Similarly, the 1911 Defense Secrets Act (in those days, the term of art was "national defense," rather than the later, broader notion of "national security") specifically mentioned only ships, forts and coastal defense facilities, and focused mainly on photographs or sketches that might aid an enemy attack. Even the draconian Espionage Act of 1917, enacted during the first flush of war hysteria and anti-German chauvinism, added only a few categories to the existing list of presumed defense secrets, such as code and signal books and information on aircraft.[10]

A number of commentators on the history of secrecy have focused – wrongly – on the World War I period as the fountainhead of modern national security secrecy.[11] Indeed, statutes such as the Sedition Act, prosecutions such as the imprisonment of Socialist Party presidential candidate Eugene Debs, roundups and deportations of "undesirable aliens" – all provide troubling parallels with the current secret detentions of Muslims, for example, in the name of counterterrorism. However, the actual national security apparatus of the time was tiny; the actual amount of secrecy regulation was minimal; and the number of secrets themselves was miniscule compared to the Cold War system. To take only one example, at the time that Secretary of State Henry

Stimson closed the U.S. "Black Chamber" codebreaking operation in 1929 and the U.S. Army quietly raised the organization from the ashes as the Signal Intelligence Service in June 1930, "America's entire cryptologic body of secrets – personnel, equipment and records – fit comfortably in a vault twenty-five feet square."[12]

While the xenophobia of World War I had revived notions of seditious libel from a century earlier – with significant implications for national security secrecy – subsequent court decisions actually strengthened freedom of the press and rights of access to government information. One of the more egregious cases involved the prosecution of Charles Schenck for his leaflets accusing Wall Street of conspiring to start World War I; Justice Holmes led the 1919 Supreme Court decision describing Schenck's words as a "clear and present danger" that Congress could prevent, but limiting the restriction on First Amendment rights to times when the nation "is at war."[13] In 1931, the Supreme Court spelled out this limitation in the landmark case of *Near v. Minnesota*, writing that in times of war

> [n]o one would question but that the government might prevent actual obstruction to its recruiting service or the publication of the sailing dates of transports or the number and location of troops.[14]

But the core ruling of *Near* applied the First Amendment to the states and dramatically expanded press freedoms by establishing the right of newspapers to criticize public officials aggressively without fear of government retribution. A subsequent Supreme Court decision in 1936 amplified this broad view, crediting the First Amendment to the prior, century-long struggle of the English people

> to establish and preserve the right ...to full information in respect of the doings or misdoings of their government," and added, "since informed public opinion is the most potent of all restraints upon misgovernment, the suppression or abridgment of the publicity afforded by a free press cannot be regarded otherwise than with grave concern.[15]

THE COLD WAR AND THE SECRECY SYSTEM

The modern system of national security secrecy in the United States arose from three sources: the initially voluntary restrictions created by the Manhattan Project scientists on nuclear weapons information as early as 1940, the total mobilization of U.S. society during World War II, and the institutionalization of these procedures in peacetime by the Cold War apparat, especially the National Security Act of 1947. Extreme deference by the courts to executive branch authority in national security matters enabled and buttressed the secrecy system, with only a handful of countervailing court or Congressional decisions. As summarized by the analyst Harold Relyea,

> with the experience of World War II and the onset of the Cold War came another permutation – the rise of the national security state. The National Security Act mandated its entrenchment. Preservation and perpetuation of the nation by any and all means have been its principle mission. Secrecy has been one of its primary characteristics.[16]

While the scientific method on its face seems the antithesis of official secrecy (think of detailed footnotes, peer review, replicable results, and race to publication), the new field of nuclear physics produced the first modern official secrecy system at the beginning of World War II. Led by refugee scientists fearful that Hitler would enslave the atom as well as Europe, physicists created a voluntary censorship program that by 1940 gained the imprimatur of the National Academy of Sciences and covered hundreds of papers and the major journals in the field. Enrico Fermi later commented,

> ...contrary to perhaps what is the most common belief about secrecy, secrecy was not started by generals, was not started by security officers, but was started by physicists. And the man who is mostly responsible for this extremely novel idea for physicists was [the Hungarian refugee Leo] Szilard.[17]

Hiding the secret of the atom from Hitler was not the only motive for official nuclear secrecy, however. The early and mostly voluntary

secrecy by the physicists soon gave way to a mammoth, formal, bureaucratic system of compartmented secrets – the hallmark of the Manhattan Project that built the U.S. atomic bomb and set the standards for official secrecy that persist even today. The Manhattan Project's "indispensable man," U.S. Army Corps of Engineers officer Leslie R. Groves, exacted unprecedented information controls not only for military and civilian government employees but also those at universities and private corporations as well. Years later, when General Groves was preparing his memoir, *Now It Can Be Told*, he wrote to his son and co-author, Richard Groves, that secrecy in the Manhattan Project had eight objectives:

> •To keep knowledge from the Germans and, to a lesser degree, from the Japanese.
>
> • To keep knowledge from the Russians.
>
> • To keep as much knowledge as possible from all other nations, so that the U.S. position after the war would be as strong as possible.
>
> • To keep knowledge from those who would interfere directly or indirectly with the progress of the work, such as Congress and various executive branch offices.
>
> •To limit discussion of the use of the bomb to a small group of officials.
>
> • To achieve military surprise when the bomb was used and thus gain the psychological effect.
>
> •To operate the program on a need-to-know basis by the use of compartmentalization."[18]

The fourth, fifth and eighth items on this list suggested the benefits to Groves of the intense compartmentation and secrecy he implemented: not only to protect national security, but also to protect his own power and influence from people who might "interfere" – such as the elected representatives of the American public. The reality of bureaucratic interest in secrecy – recognized a century ago by the sociologist Max Weber, who described secrecy and regulation as the core behaviors of bureaucracies – should serve as a caution against accepting every government claim of national interest. Yet the early Cold War set a pattern of doing just that.

The Manhattan Project's approach carried over into peacetime with the Atomic Energy Act of 1946, later amended in 1954 to allow for controlled involvement of private industry in the nuclear business, and for the Atoms for Peace program spreading nuclear energy capability around the world. These statutes established the principle that nuclear information is "born classified" – defined as "Restricted Data" and including controls "that went beyond those ever imposed by Congress, before or after."[19] The Smyth Report, issued within a week of the Hiroshima bomb, had explained the work of the Manhattan Project for the historical record, and attempted to establish the boundaries of what information could be released and what kept secret. Critics at the time and since (as recently as the hysteria over Chinese nuclear spying in the 1990s) have alleged that the Smyth Report and other such declassifications gave away crucial secrets to our nation's adversaries. The czar of nuclear secrecy, General Groves, thought otherwise:

> The big secret was really something that we could not keep quiet, and that was the fact that the thing went off. That told more to the world and to the physicists and the scientists of the world than any other thing that could be told to them. It was something that we did not know until we had spent almost $2,000,000,000 and had worked about three years. We did not know whether it would go off or not, and that is the thing that really told them more than anything else that could be told.[20]

Parallel to the institutionalization of the secret nuclear bureaucracy came the formation of the rest of the national security state. The National Security Act (NSC) of 1947 set up the National Security Council to coordinate defense, foreign, and intelligence policies, and the Central Intelligence Agency as the President's permanent spy service, with the primary mission of preventing another Pearl Harbor. The open legislative process that established these entities soon gave way to covert processes. Among the earliest policy directives of the NSC were secret orders for the CIA to intervene in the 1948 Italian elections, and to wage clandestine anti-Soviet operations ranging from propaganda to sabotage. The 1947 Act gave the CIA director open-ended authority to

protect "sources and methods" of intelligence, while a 1949 statute cloaked the CIA's budget; and the "black" agencies proliferated: President Truman created the communications-intercept agency, the National Security Agency, in 1952, and President Kennedy in 1961 added the National Reconnaissance Office, the very existence of which was classified until 1992.[21]

Only after Watergate and Vietnam, when Congress finally investigated the intelligence agencies, did the American public learn what secrecy of "sources and methods" covered up. The Church Committee summed up Cold War secrecy in 1976, with its questions:

> What is a valid national secret? Assassination plots? The overthrow of an elected democratic government? Drug testing on unwitting American citizens? Obtaining millions of private cables? Massive domestic spying by the CIA and the military? The illegal opening of mail? Attempts by the agency of a government to blackmail a civil rights leader? These have occurred and each has been withheld from scrutiny by the public and the Congress by the label "secret intelligence."[22]

The secrecy attending intelligence matters also became the norm for presidential directives on national security. Between 1961 and 1988, only 247 out of 1,042 such directives issued through the NSC were also publicly released. By the 1980s, members of Congress were complaining about "secret law," and pointing to specific examples of directives that seemed designed to evade Congressional intent. Other examples from directives that have since been declassified included statements such as "The Middle East Peace Process, in which progress must be achieved as rapidly as feasible" – these words were classified Secret for years – or "maintain high confidence that our second strike capability is sufficient to deter an all-out surprise attack on our strategic forces" – classified Top Secret even though obvious. To this day there exists no formal mechanism for public notice of these directives; and the White House refused to release the text of President George W. Bush's very first such directive, on the reorganization of the NSC, until a copy leaked and the press reported that the document was actually unclassified.[23]

The security classification system found its charter in a different series of directives, executive orders issued by presidents from Truman to George W. Bush. The first executive order on classification, in 1951, changed the words "national defense" to "national security." (Around the same time, the Invention Secrecy Act of 1952 authorized the government to classify private patents, an action from which there was no recourse for the inventor.) The sequence of executive orders on secrecy featured an unlikely standout – President Nixon's – which imposed real limits on the bureaucracy including the first sunset terms for secrecy duration, the first prohibition on classification to conceal error or embarrassment, and the first requirement to "portion mark" documents so that unclassified portions could be released. Nixon's motivations hardly centered on true openness, however; he saw the bureaucracy as a nest of holdover Democrats and spent hours (documented in the White House tapes) musing about new forms of classification for the President's eyes only. In the same July 24, 1971 conversation with staffers John Ehrlichman and Egil Krogh (later the head of the infamous Watergate "plumbers" who started out as pluggers of leaks) in which the President referred to future Chief Justice William Rehnquist and his Justice Department group working on the new executive order as "Renchburg" and "that group of clowns," Nixon led the following discussion:

President:	And maybe another approach to it would be to set up and remember I already mentioned to set up a new classification.
Ehrlichman:	Right.
President:	Which we would call what? Let's just call it a new classifica – Don't use TOP SECRET for me ever again. I never want to see TOP SECRET in this god damn office. I think we just solved – shall we call it – uh, John, what would be a good name? "President's Secure" – or, uh, "Eyes Only" is a silly thing, too. It doesn't mean anything any more. Uh –
Krogh:	We used "Presidential Document" before with one of the counsel we were working with, but that didn't – there's some –

Ehrlichman: How about – uh, uh, looking forward to the court case, I wonder if we could get the words "National Security" in it.

President: Yeah.

Ehrlichman: So that "National" uh, just say "National Security Classified" or "National Security –"

Krogh: [Unintelligible]

Ehrlichman: "Secret" or uh –

President: Well, uh, not the word "Secret" should not be used.

Ehrlichman: All right, uh, uh –

President: Because you see "Secret" has been now compromised.

Ehrlichman: How about "Privilege"?

President: "Privilege" is, is not strong.

Ehrlichman: Too soft, too soft.

President: "National Security" uh, "National Security" uh –

Ehrlichman: "Restricted." "Restricted."

President: Right. "National Security" and uh, I agree to "National, Na – , National Security" –

Ehrlichman: "Restriction"?

President: "Priority."

Ehrlichman: "Controlled"?

President: Or "National Security – Priority – Restricted – Controlled."

Ehrlichman: Oh, we'll – let us work on it.[24]

The low point of executive orders on secrecy was probably President Reagan's order, which turned the secrecy system into the land of the midnight sun, leaving the duration of secrets up to the originating agency and thus leaving to his successors a mountain range of unnecessary secrets. Some of the Reagan era initiatives for increased secrecy were blunted by the Congress, but the new role of the Office of Management and Budget in constricting government publication of information combined with a series of Justice Department initiatives tightening the application of the Freedom of Information Act – in fact, attempting to exempt whole agencies from the reach of the law, and successfully doing so for the "operational files" of the CIA – dramatically increased government secrecy in the 1980s. The best summary of these developments gave the bottom line in its title: The American Library Association's award-winning chronology featured as its running title, Less Access to Less Information. [25]

Enabling the government's secrecy addiction was a deferential judiciary. Over the course of the Cold War, the U.S. government adopted and the Supreme Court ratified any number of restrictions on openness in the name of protecting national security. The only exceptions to the general rule of court deference to executive national security claims occurred when the underlying substance of the information in dispute involved major scandal (the contents of the Nixon White House tapes, for example) or a highly disputed government policy with sinking public opinion ratings (the Vietnam War history in the Pentagon Papers). The latter case, which the Supreme Court decided 6-3 in 1971 with a brief *per curiam* opinion against any prior restraint on publication, produced the only ringing endorsements of openness available from a Supreme Court majority – undermined by the fact that each Justice wrote a separate opinion because of the rushed schedule. For example, Justice Potter Stewart pronounced:

> In the absence of governmental checks and balances present in other areas of our national life, the only effective restraint upon executive policy and power in the areas of national defense and international affairs may lie in an enlightened citizenry – in an informed and critical public opinion which alone can here protect the values of democratic government.[26]

Unfortunately, before the decade of the 1970s was out, Justice Stewart had forgotten those strong words and rejoined the tradition of judicial support for executive secrecy. According to internal Supreme Court documents later found in the Thurgood Marshall papers, Stewart and

Chief Justice Warren Burger were the first two members of the Court to join Justice Lewis Powell's *ad hominem* attack in November 1979 on former CIA agent Frank Snepp, whose book *Decent Interval* had exposed official dereliction during the final days of the Vietnam war. At the CIA's urging, the Justice Department had sued Snepp for not submitting the manuscript to the CIA for clearance before publication, and won the case before a biased district court judge who did not allow Snepp's lawyers to pursue the fact that Snepp had revealed no classified information. When the case reached the Supreme Court, Justice Powell persuaded his brethren to go beyond the Court of Appeals decision in the case, and authored the unsigned *per curiam* opinion issued on February 19, 1980. The Court shamefully imposed a constructive trust on Snepp's earnings from the book, enjoined him from publishing without clearance from the CIA, and effectively placed the legal status of an employment contract above the First Amendment, without even considering the interaction of the two and without any evidence that Snepp had revealed classified information. The Court rendered the *Snepp* decision without allowing written or oral argument, in a rush to judgment that ignored the available record, apparently under the influence of hostility to the concurrent publication of the Bob Woodward/Scott Armstrong best-seller *The Brethren*, which revealed the Court's inner workings based on interviews with former clerks.[27]

The government's secrecy claims in the Pentagon Papers case did persuade three Justices to rule against the plain language of the First Amendment, and thus provides a particularly instructive test of national security secrecy. The Solicitor General of the United States, Erwin Griswold, believed that a general claim of classification was not enough, given factual findings of the lower courts involved that various specific items in the Papers had previously been officially acknowledged. And Griswold had no time to read the 47 volumes himself. So he made security officials identify the "drop dead" secrets (they claimed 40 items, of which Griswold only agreed on eleven) for a formal brief – itself classified – to the Supreme Court. Using the public record and declassified (but still partially censored) versions of the government's secret brief, an item by item comparison by the scholar John Prados for the National Security Archive on the 30th anniversary of the case demonstrated that none of Griswold's eleven "drop dead" secrets was truly damaging to U.S. national security.[28]

Interestingly, Griswold himself had already come to the same conclusion:

> I have never seen any trace of a threat to the national security from the publication. Indeed, I have never seen it even suggested that there was such an actual threat....It quickly becomes apparent to any person who has considerable experience with classified material that there is massive overclassification and that the principal concern of the classifiers is not with national security, but rather with governmental embarrassment of one sort or another. There may be some basis for short-term classification while plans are being made, or negotiations are going on, but apart from details of weapons systems, there is very rarely any real risk to current national security from the publication of facts relating to transactions in the past, even the fairly recent past.[29]

At the time of the Supreme Court argument, however, Griswold made the opposite case, and the three Supreme Court votes he won to restrain publication of the Pentagon Papers were much more typical of the Court's jurisprudence during the Cold War than was the actual outcome of the Pentagon Papers case. The height of judicial deference probably occurred in the 1953 case of *United States v. Reynolds*, which set the modern standard for the "state secrets" privilege. In a civil action brought by the widows and families of those killed in a 1948 crash of an Air Force B-29 Superfortress, the Court refused to compel the government to turn over the crash reports, declined to review the documents at issue, and deferred completely to affidavits from the Secretary of the Air Force, Thomas K. Finletter, and the Air Force Judge Advocate General, Major General Reginald Harmon, who claimed under oath that the crash investigation documents would reveal national security secrets about electronic equipment the plane was carrying – secrets so sensitive that the courts could not see them. The Court set the standard this way:

> [W]hen the formal claim of privilege was filed by the Secretary of the Air Force, under circumstances indicating a reasonable possibility that military secrets were involved, there was certainly a sufficient showing of privilege to cut off further demand for the documents....

Nearly 50 years later, the daughter of one of the plaintiffs discovered through Internet research that the documents had been declassified, and upon reading them, found no details of secret electronic equipment, only repeated acts of negligence by the Air Force that had led to the airplane's engines catching fire. In other words, the Reynolds precedent – cited in more than 600 subsequent cases and the basis for dismissal for multiple whistleblower cases – rose directly from government fraud and lies.[30]

Similarly, the single most egregious violation of American civil liberties in modern times – the internment of 120,000 Japanese-Americans during World War II – secured deference, indeed endorsement, from the courts based in significant part on false claims of military necessity. Professor Peter Irons of the University of California at San Diego used the Freedom of Information Act in 1982 to obtain Justice Department documents on the key internment prosecution, *Korematsu v. United States*, decided for the government by the Supreme Court in 1944. Irons' documents encouraged Fred Korematsu to sue to vacate his conviction on grounds of government misconduct; and in fact, in 1984 a federal district court did so, finding that

> the government knowingly withheld information from the courts when they were considering the critical question of military necessity in this case.

Judge Marilyn Patel concluded with this warning about the Supreme Court's 1944 decision: "Korematsu remains on the pages of our legal and political history. As a legal precedent it is now recognized as having very limited application. As historical precedent it stands as a constant caution that in times of war or declared military necessity our institutions must be vigilant in protecting constitutional guarantees. It stands as a caution that in times of distress the shield of military necessity and national security must not be used to protect governmental actions from close scrutiny and accountability. It stands as a caution that in times of international hostility and antagonisms our institutions, legislative, executive and judicial, must be prepared to exercise their authority to protect all citizens from the petty fears and prejudices that are so easily aroused."[31]

Griswold, *Reynolds*, and *Korematsu* to the contrary notwithstanding, the current Chief Justice of the U.S. Supreme Court remains locked in deference to, not skeptical scrutiny of, government secrecy claims. In a 1998 magazine article and book (*All the Laws But One: Civil Liberties in Wartime*), Justice William Rehnquist actually sought to justify the military's role in the Japanese-American internments. Rehnquist wrote:

> In defense of the military it should be pointed out that these officials were not entrusted with the protection of anyone's civil liberty....

Actually, each military officer takes the same oath that Rehnquist administers to Presidents, that they will "support and defend the Constitution." Rehnquist consigned to academics the question of

> whether occasional presidential excesses and judicial restraint in wartime are desirable or undesirable" and claimed "no reason to think that future wartime Presidents will act differently from Roosevelt or that future Justices of the Supreme Court will decide questions differently from their predecessors.[32]

Contrary to Rehnquist, there have been at least a dozen examples of lower courts ruling against the executive on national security grounds. Even though most were reversed on appeal, some were not, and there are hundreds of examples of Freedom of Information Act (FOIA) cases for national security data in which – although the ultimate judgment went for the government – along the way the FOIA requester successfully obtained much of the information sought.[33] The FOIA did not originally allow for requesters to challenge national security secrecy claims, since a *Reynolds*-style standard governed requests before Congress adopted the 1974 FOIA amendments. These amendments specifically reversed the one Supreme Court FOIA case on national security, the 1973 decision in *EPA v. Mink*, in which members of Congress sought nuclear testing records because of environmental concerns. The Court held that the FOIA provided no judicial review of classification decisions. In a major victory for openness, the Congress rejected this notion in 1974, as well as the Ford administration's view that court review should be limited only to determining whether there was a "reasonable basis" for the classification. It was no coincidence

that this high-water mark for openness coincided with the height of the Watergate scandal and President Nixon's forced resignation from office. The 1974 amendments still accorded "substantial weight" to agency affidavits, but encouraged "in camera" examination of the withheld records in dispute. Despite the clear language of the legislative history, some courts have employed language like "utmost deference" and, unfortunately, the general tendency of federal judges is to apply exactly the "reasonable basis" standard that was rejected by Congress.[34]

A more comprehensive treatment of national security secrecy than this paper can muster would include discussion of various attempts by Congress to open national security information in limited ways for specific public purposes during the Cold War. For example, the Arms Export Control Act, first passed as the Foreign Military Sales Act in 1968 and strengthened significantly in 1972 after controversy over arms shipments to Iran by the Nixon administration, compelled reporting to Congress and to a certain extent, the public, on American sales of weapons abroad. Responding to revelations about a series of spies who were never prosecuted because to do so the government would have to reveal secret "sources and methods," the Congress in 1980 enacted the Classified Information Procedures Act to create pretrial procedures such as unclassified summaries of evidence that would allow trials to proceed and defendants to confront the evidence and their accusers, without giving away the specifics of the underlying intelligence collection method or other sensitive information.[35]

But the real story of national security secrecy during the Cold War was the mountain range, the paper Himalayas, of secrets created by the classifiers. Inside experts charged with monitoring the system admitted they could not precisely measure how many secrets the government held. The 1997 Moynihan Commission estimated that some 1.5 billion pages that were 25 years or older were still classified by the federal government as of 1997. Pursuant to a mandate from Congress, the Office of Management and Budget did begin in the 1990s to collect information on the costs of keeping all these secrets. One industry estimate in 1989 put the annual total just among government contractors as $13.8 billion – all of which was covered by taxpayer dollars, of course. A more recent estimate reported that the costs related to protecting national security information in both industry and government amounted to over $5.6 billion in 1995.[36]

A wider spread of disagreement persisted on the point that Erwin Griswold raised: the degree of overclassification. The internal watchdog agency, the Information Security Oversight Office, consistently estimated during 1990s that only between one and ten per cent of classified records should not be classified. Yet in 1991 the career Navy officer and Executive Secretary of President Reagan's National Security Council, Rodney B. McDaniel, estimated that only 10 per cent of classification was for "legitimate protection of secrets."[37] The Moynihan Commission report gave multiple examples, ranging from classifying all the support functions related to classified weapons systems, to a "family day" memo to agency staff that was classified because the signer was from the covert operations side of the agency, or briefing slides that were classified but the briefers could only answer "I'm not sure" and "This is just the way we prepare our materials" when asked why.

THE "DECADE OF OPENNESS" AND THE BEGINNING OF RETRENCHMENT

The end of the Cold War began the "decade of openness," as history will describe those years between the collapse of the Soviet Union and the collapse of the World Trade Center towers. There were many highlights in U.S. national security information policy. Under President George H.W. Bush in 1991, then-CIA director Robert Gates launched a "CIA openness" project, a name he acknowledged as an oxymoron. Unfortunately for his public relations, the task force report recommending the openness project was itself classified Secret, until a Freedom of Information Act Request and public embarrassment forced its release. The CIA's motivations included refuting those critics who accused it of missing the implosion of the Soviet Union, and improving its image with Capitol Hill and the public (citing the Efrem Zimbalist Jr. TV series on the FBI as an example to emulate). But the report's bottom line was *"Preserve the mystique*."[38] More substantive releases came from President Clinton's responsiveness to document requests from truth commissions in El Salvador and Guatemala, and from human rights advocates after the arrest of former Chilean dictator Augusto Pinochet – White House staff overrode intelligence community objections and forced the declassification of documents that had been withheld from FOIA releases.[39]

Congress passed new laws mandating openness in the early 1990s, of which two stand out for proving that secrecy is too important to be left to the securocrats. A 1991 law established a formal committee of outside historians to ensure that the State Department's documents publications on the history of U.S. foreign relations were accurate and complete. A 1989 volume on U.S. relations with Iran in the 1950s had somehow (at the behest of the CIA) managed to leave out any mention of the CIA-organized coup against the Mossadegh government in 1953, and the head of the previous, purely advisory historians' committee had resigned in protest. With a new statute backing them up, the State Department committee soon became key advocates for declassifying covert operations documents and other icons of the secrecy system.[40] Another new statute responded to the hit movie "JFK," which alleged a grand conspiracy among the CIA and the military-industrial complex to assassinate President Kennedy and gained what mainstream credibility it had from the fact that so much remained secret from CIA and other files about Lee Harvey Oswald and the assassination investigations. The new law set up an independent panel, the Assassination Records Review Board, headed by a state deputy attorney general (later a federal judge) and included three historians and a librarian, who successfully obtained the declassification of more than four million pages of previous secrets – usually over intelligence community objections.[41]

Several of President Clinton's executive orders on secrecy set remarkable new precedents. In 1994, the President ordered the release of more than 40 million pages of secret documents dating back to World War I through the Vietnam War – documents that had languished in classified files despite the improbability that they contained intelligence sources and methods or weapons system designs. In a 1995 innovation, President Clinton reversed the tendency toward ever-increasing secrecy, by ordering sunsets and specific justifications on each secret, together with a practice called automatic declassification, which allowed many documents, based on their age and subject matter and a sampling methodology, to be declassified with minimal and low-cost review. In the first five years of the order, federal agencies declassified an extraordinary, almost unimaginable 800 million pages of previously secret government records, according to the federal Information Security Oversight Office – more than all other U.S. Presidents combined had ever ordered declassified. Another executive order started the declassification of more than 800,000 spy satellite images from the Cold War,

with specific mention of their utility to environmental scientists looking at topics like global warming.[42]

Three dynamics slowed and ultimately stopped this cascade of openness by the end of the 1990s. First, Republican partisans in control of the Congress sought revenge for Clinton's 1996 re-election victory by chasing wisps of conspiracies involving Chinese political contributions and nuclear secrets (a form of security hysteria that reached its peak with the botched espionage prosecution of Los Alamos scientist Wen Ho Lee). Second, the CIA's brief period of attempting greater openness ended with the arrest of double agent Aldrich Ames, who had betrayed numerous CIA assets in Russia; and the CIA reverted to its normal hyper-security. Finally, in 1998 President Clinton went on the defensive in the Monica Lewinsky affair, and ultimately avoided impeachment by only 10 votes in the Senate.

By 1999, retrenchment was in full swing. Following reports that some sensitive nuclear weapons information had been inadvertently released in the declassification process, agencies requested and Congress approved a special screening effort to prevent such releases. "Only about ten percent of the files awaiting declassification potentially contain[ed] misfiled nuclear secrets" and therefore warranted closer scrutiny, according to the head of the ISOO, career official Steve Garfinkel. Nevertheless, with Congressional backing, many agencies insisted on performing a detailed, page-by-page review of all of their records, drastically slowing the declassification process while providing a form of full employment for securocrats. At the same time, in one of the most bizarre moves of retrenchment, the U.S. Space Command on March 1, 1999 stopped providing unclassified tracking information on military satellites – information that had been public for many years – even on the 24 Global Positioning System satellites whose very function is to broadcast their locations to GPS users such as merchant ships and surveyors.[43]

Under pressure from Freedom of Information litigation, the CIA had disclosed for the first time in 1997 the size of the total U.S. intelligence budget ($26.6 billion), and subsequently released the 1998 number as well ($26.7 billion). President Clinton had informed Congress he would not object to such a budget declassification since the release

would not damage national security. But in late 1998, just as the House of Representatives voted to impeach President Clinton, CIA director George Tenet announced he would not disclose the 1999 budget total, claiming that to do so would place the United States at risk. Since there was nothing that Slobodan Milosevic or Saddam Hussein could have done with such information, the CIA was actually reducing the risk of a public debate here in the U.S. over the probable increases the 1999 number would have revealed. In a reversion to Cold War practice, a federal court then upheld the CIA's decision; and the litigation continued, with the CIA fighting a followup FOIA lawsuit seeking the 1947 budget number, just to prove the absurdity of the national security claim.[44]

All of this is not to say that the concerns over security that dominated the public debate in the late 1990s were completely illegitimate. No American citizen favors the release of sensitive information that could facilitate the spread of nuclear or chemical weapons, for example, or that could jeopardize U.S. pilots flying missions abroad – all of which is appropriately classified secret. But the security frenzy of the late 1990s tellingly targeted public access to unclassified information and the entire declassification program – not the occasional inadvertent disclosure – thus exposing the larger agenda of secrecy reform rollback. If inadvertent disclosure of nuclear information were the real issue, the securocrats would have produced a focused cost-effective plan for reviewing just those records most likely to contain misfiled nuclear weapons data. And the plan would have applied new post-Cold War standards to the historical documents awaiting review, not simply replicating the aggressive secrecy rubber-stamping of the past that so vastly overclassified government information at such great cost to taxpayers. The securocrats themselves admit, like General Groves, that no classification program can close off technological and scientific secrets for more than a limited time. On nuclear weapons, for example, we now know the Soviet Union was only two years away from a home-grown atomic bomb when it exploded its 1949 bomb based on stolen American designs.[45] The point of nuclear secrecy, ever since the Manhattan Project, had been simply to raise the costs to potential adversaries and would-be proliferators. But in the case of the rollback at the end of the Openness Decade, it was primarily the costs to the public that were going up. And then the Bush administration arrived.

THE IDEOLOGICAL ORIGINS OF BUSH ADMINISTRATION SECRECY

The Bush administration's obsession with secrecy began well before September 11th, and it did not arise from the war on terrorism. Rather, the ideological origins of the secrecy fetish for this White House lie in the battles over presidential power that Presidents Nixon and Ford lost in the 1970s. President Bush and Vice President Cheney do sincerely believe that the American people have made the White House way too open, way too accountable, over the past 30 years since Vietnam and Watergate. One might say that this administration is trying to haul those pesky open government laws off to the secure, undisclosed location where they've been keeping the Vice President. Perhaps the most illuminating single conversation on this subject occurred in January 2002, on ABC News "This Week," when ABC's Cokie Roberts asked Vice President Cheney about his energy policy task force, whose documents and even the names of the members Cheney had refused to give Congress, the General Accounting Office, or the public. Roberts queried,

> These things generally end up with people turning over the papers. The Republicans are dying to have you turn over the papers. Why not turn over the papers?... It looks like they're hiding something.

Cheney began by saying that withholding the information was where "the lawyers decided" to draw the line, then he went on to give his core belief:

> But in 34 years, I have repeatedly seen an erosion of the powers and the ability of the President of the United States to do his job ... We've seen it in cases like this before, where it's demanded that the president cough up and compromise on important principles... unwise compromises that have been made over the last 30 or 35 years."[46]

Some 35 years ago, of course, was the first version of the U.S. Freedom of Information Act, passed by Congress in 1966 and signed, grudgingly, by President Johnson whose signing statement emphasized as much the need for secrecy as for openness. The law only acquired teeth with

the 1974 amendments, enacted in the wake of Watergate, or, again on the Cheney time scale, almost 30 years ago. Those 1974 amendments were a defining experience for the new White House deputy chief of staff, a 34-year-old in his first really big job in Washington – named Richard Cheney. He reported to a more experienced Washington hand, a former Congressman named Donald Rumsfeld, chief of staff to President Ford; and their first big challenge was to keep President Ford's veto of the 1974 amendments from being overridden by Congress. The Ford objection was straightforward: the President, Rumsfeld, Cheney and their lawyers believed that any law that could force the President to release information he didn't want to release was unconstitutional, particularly on national security grounds.[47] Ironically, Rumsfeld had been the original Republican co-sponsor of the Freedom of Information Act in 1966. He spoke ringing words at the time on the floor of the House of Representatives:

> [D]isclosure of government information is particularly important today because government is becoming involved in more and more aspects of every citizen's personal and business life, and so access to information about how government is exercising its trust becomes increasingly important.[48]

But at the time Rumsfeld spoke, the President was a Democrat. When Democrats first drafted a freedom of information law, in the 1950s, the President was a Republican and no Republican member of Congress signed on. By 1966, the President was a Democrat, and all of a sudden it was in the interest of Republicans to hold the executive accountable – thus Rumsfeld's support. In 1974, the tables were turned; one Republican President had resigned in disgrace, his successor faced a Congress controlled by the opposition; but all President Ford needed to sustain his freedom of information veto was one third of the Senate. Congressional advocates of FOIA had tried to avoid a veto, engaging in a series of negotiations over the bill's language with agencies like the FBI. According to an FBI document later released under the Freedom of Information Act, both the Nixon and Ford administrations had been expecting to use a veto. A June 17, 1974 FBI memorandum conveyed internal orders from the White House legislative affairs office that there should be no more negotiations with Senate staff for compromise on the FOIA amendments. The FBI memo said "they want no changes made

in this legislation since they want it to remain as bad as possible to make their case stronger for sustaining a certain veto."[49]

But Congress overrode the Ford veto, and the 1974 amendments are the core of the U.S. Freedom of Information Act today.

That the open government laws of the 1970s were "as bad as possible" is an attitude that permeates the Bush administration today. Many of the current battlegrounds for openness center around statutes, like the Presidential Records Act, that were offspring of the Watergate scandal. And on the broader question of national security information, the Ford-Rumsfeld-Cheney position lives on. President Bush is an absolutist, repeatedly asserting unilateral power to withhold information even from the Congress. For example, in the October 23, 2002 signing statement for the fiscal year 2003 defense appropriations bill, President Bush declared:

> The U.S. Supreme Court has stated that the President's authority to classify and control access to information bearing on national security flows from the Constitution and does not depend upon a legislative grant of authority.[50]

This is, of course, not the whole story. As the 1997 Report of the Commission on Protecting and Reducing Government Secrecy concluded,

> the Necessary and Proper Clause in Article I, section 8, of the Constitution, which grants the Congress the authority to 'make Rules for the Government and Regulation of the land and naval forces,' provides a strong basis for Congressional action in this area. As an area in which the President and the Congress 'may have concurrent authority, or in which its distribution is uncertain,' the security classification system may fall within the 'zone of twilight' to which Justice Robert H. Jackson referred in 1952 in his famous concurring opinion in *Youngstown Sheet and Tube v. Sawyer* (the 'steel seizure' case)."[51]

MAPPING THE BATTLEGROUNDS OF THE INFORMATION WAR

Theology is not the whole story, of course. As General Groves let slip in his 1958 list of reasons for nuclear secrecy, control of information keeps people (like Congress, other bureaucrats, nosy reporters, or critical voters) from interfering with your program. The grave danger to openness today in the United States comes from the combination of secrecy theology at the highest levels and at all levels the bureaucratic imperative. The primary battles in the current information war are raging exactly along these front lines of presidential authority and bureaucratic control. Before September 11th, the Bush administration had already drawn the line on access to presidential and vice-presidential records. Vice President Cheney not only withheld his energy task force documents, but also persuaded a federal court to throw out a lawsuit by the General Accounting Office (GAO) seeking those records, on the grounds that GAO had not exhausted its Congressional options for getting the documents. However, with the Congress now dominated by Republicans, GAO actually had and has no such options. The case also produced a small victory for the Freedom of Information Act, since a separate legal action under the FOIA actually produced a number of the task force documents in the files of the Department of Energy.[52]

The other prominent example of pre-September 11th secrecy targeted the Presidential Records Act. A routine release of 68,000 pages of Reagan-era records landed on the new White House Counsel's desk in January 2001, and instead of letting the release go forward (as four million pages of Reagan White House documents had already done), the White House stalled. Ultimately, in November 2001, the White House issued a new executive order that turned the Presidential Records Act on its head – giving former Presidents and even their heirs the indefinite ability to stall release of their records. Curiously, the first former Vice President to receive executive privilege on his own was the incumbent President's father. A lawsuit by historians and public interest groups to prevent the National Archives from implementing the order is pending in federal district court.[53]

One significant secrecy change actually bridged the period before and after September 11th. Attorney General John Ashcroft issued a formal

memorandum on October 12, 2001, which had been in the works for months, reversing a Clinton administration policy of encouraging disclosure of information under the Freedom of Information Act. The Clinton policy, articulated in formal memos to agencies from President Clinton and from Attorney General Janet Reno in 1993, urged openness even when the information involved might be technically covered by a FOIA exemption, unless there was "identifiable harm" from the release that outweighed public interests in openness. In contrast, the Ashcroft memo told agencies that if they could find any "reasonable basis," legal, technical, or whatever, to withhold documents under the freedom of information act, they should go right ahead and the Justice Department would back them up. The Ashcroft memo barely mentioned national security, but a subsequent audit of federal agencies showed the greatest impact of the memo occurred at the Army, Navy and Air Force.[54]

The shock of the September 11th terrorist attacks precipitated a wide range of actions designed to prevent information from reaching the public. Rhetoric denouncing leaks and emphasizing secrecy even for unclassified information emanated from President Bush, Vice President Cheney, Secretary of Defense Rumsfeld, Deputy Secretary of Defense Wolfowitz, and many other high officials. Some of the new secrecy moves were old wishlist items of the bureaucracy, such as the expanded surveillance authority included in the so-called USA Patriot Act. Most dramatically, the federal government began a massive roundup of Muslim Americans, totaling over 1300 secret arrests in all. Attorney General Ashcroft refused to name the detainees, asserting not only that to release the names would give Al Queda some kind of roadmap to the investigation, but more speciously, that the Justice Department was protecting the detainees' privacy. Yet on the few occasions when the government made arrests of people actually connected to Al Queda, not only their names were trumpeted to the media, but cameras were invited along on the arrests. In the FOIA case brought to obtain the names of the detainees, U.S. district judge Gladys Kessler ruled for the plaintiffs in August 2002, finding that "secret arrests are a concept odious to a democratic society." Plaintiffs in the case now believe that the most likely reason for the continued secrecy on the secret arrests is to cover up the reality that few or none were actually connected to terrorism. The roundup was a lashing-out by law enforcement officials led by Attorney General John Ashcroft, who could not think of anything else to do.[55]

Ashcroft has become a kind of poster child for the rollback of openness, with his name firmly affixed both to the FOIA memo and more importantly, to the secret arrests. A particularly defining moment came in early December 2001, during Congressional testimony by the Attorney General, defined the debate as between terrorism fighters (like himself) and terrorists, between hawks and doves, between more secrecy and aiding and abetting the enemy. Ashcroft told the Senate Judiciary Committee:

> To those who scare peace loving people with phantoms of lost liberty, my message is this: Your tactics only aid terrorists, for they erode our national unity and diminish our resolve. They give ammunition to America's enemies and pause to America's friends.[56]

This kind of thinking produced what Senator Patrick Leahy (D-Vt.) described as the "most severe weakening of the Freedom of Information Act in its 36-year history" – the "critical infrastructure information" exemption in the 2002 Homeland Security Act. This provision, originally drafted by the Bush administration and enacted in a last-minute midnight process in place of a bipartisan compromise, essentially gave companies that voluntarily share information with the government about their vulnerabilities not only the promise of confidentiality, but also immunity from civil liability if the information revealed wrongdoing. Senator Leahy accurately characterized the provision as "a big business wish list gussied up in security garb."[57]

The most difficult case for openness advocates occurred as the result of a newspaper article, but it illustrates both the vulnerabilities of an open society and the use of openness to fix those vulnerabilities. On January 13, 2002, *New York Times* reporter William Broad published a front page story titled "U.S. Selling Papers Showing How to Make Germ Weapons." Broad discovered that anyone could order a copy from the government of bioweapon "cookbooks" that had been declassified years earlier. The story sparked a White House memorandum (signed by chief of staff Andrew Card on March 19, 2002) that asked agencies to review all their publicly available data for similar information that would help terrorists acquire weapons of mass destruction. In the context of an overall Bush administration push towards greater secrecy, the

Card memo contributed to a knee-jerk response: After September 11th and before the Card memo, government agencies had already pulled more than 6,000 documents from Web sites, according to the Federation of American Scientists, including some that had no national security implications, such as the Pentagon's evaluation reports on procurement programs – not something a terrorist could use in any way.[58] Few realized that the issue would never have been highlighted without the public's access, through a newspaper reporter, to the vulnerability of the information.[59]

The problem in the Bush administration is their first instinct is to suppress the information about hazards, instead of addressing the hazards directly. The Environmental Protection Agency has pulled data from their web site about the locations of chemical plants and storage. Indeed, no one is in favor of giving terrorists a target list. But then look what happens in real life. A *Baltimore Sun* reporter goes and digs up the data from before the EPA site was censored, and finds out that right down next to the harbor, in the middle of some poor neighborhoods where thousands of people live, are tanks full of chlorine that in case of fire would turn right into poisonous gas. Only after she writes her story do the chemical companies change the mix in those tanks and disperse the chlorine. So does pulling the information really protect us? Now the Federal Aviation Administration is pulling all the public reports of its airport fines for security violations. Sounds reasonable, except now who's going to make sure the FAA does its job?[60]

THE NEW PARADIGM – OPENNESS IS SECURITY

A new paradigm is struggling to emerge from the ashes of the World Trade Center. Originally, this paradigm had nothing to do with terrorism but came directly from the scientific method – tested hypotheses, complete citations, replicable results, peer review. The most articulate exponents of openness – even and particularly in the new Cold War hothouse of nuclear secrets – were precisely the scientists who had developed the Bomb, and they argued not so much on behalf of democratic values, or civil rights and liberties, but on scientific efficiency, and national security. Vannevar Bush, for example, President Roosevelt's key science adviser during World War II, stated the following in 1945: "Our ability to overcome future enemies depends upon scientific

advances which will proceed more rapidly with diffusion of knowledge than under a policy of continued restriction of knowledge now in our possession."[61]

The Tolman Committee appointed by General Groves in 1945 to assess any declassification of Manhattan Project information, stated its general philosophy as follows:

> It is not the conviction of the Committee that the concealment of scientific information can in the long-term contribute to the national security of the United States. It is recognized that at the present time it may be inevitable that the policy of the Government will be to conceal certain information in the interest of national security. Even within this limitation there are many matters whose declassification would greatly help the progress of science without violating that policy. If we are looking to the national welfare or national security as they may be two decades from now the Committee has no doubt that the greatest strength in both fields would come from a completely free and open development of science. Thus, the Committee is inclined to the view that there are probably good reasons for keeping close control of much scientific information if it is believed that there is a likelihood of war within the next five or ten years. It is also their view, however, that this would weaken us disastrously for the future – perhaps twenty years hence.[62]

A more modern iteration of the same analysis came from Dr. Edward Teller, co-inventor of the hydrogen bomb and avatar of ballistic missile defense. Teller wrote *The New York Times* in 1973:

> I urge the United States to move…toward unilaterally abandoning all forms of scientific and technical secrecy….I advocate this in the enlightened self-interest of the United States… First [because] in science there are very few real secrets…. Second [because of] the long term [adverse] effects of secrecy on scientific progress, especially in the United States.[63]

The most current critique of secrecy in the United States rises directly

from the lessons of the September 11th terrorist attacks. During the Congressional hearings on what went wrong in law enforcement that otherwise might have prevented the attacks, the Immigration and Naturalization Service and the Federal Aviation Administration testified that excessive secrecy was the problem. The intelligence agencies and particularly the CIA had not shared with either the INS or the FAA the urgency of searching for the two September 11th hijackers who were living in the U.S. and booked their September 11th tickets under their own names. "Had we had information that those two individuals presented a threat to aviation or posed a great danger, we would have put them on the list and they should have been picked up in the reservation process," the Transporation Security Administration testified.[64]

One of the leaders of the 1990s retrenchment began singing a new tune. Sen. Richard Shelby (R-Alabama), apparently saw no contradiction between his role as chief sponsor of the proposed "official secrets act" that was vetoed by President Clinton, and his minority report critique of the CIA's information "hoarding" as one of the underlying causes of the intelligence failures leading to September 11th. According to one *Washington Post* reporter who paid attention to Shelby's gripes, some of the hoarding occurred because the intelligence agencies didn't have the technology to make sharing possible. Some took place because they didn't even know what they had in their own case files and on their intercept tapes. And some came because they thought certain secrets were too sensitive to share, either to protect sources and methods, or preserve their own unique standing in the intelligence pecking order. Shelby wrote:

> This is particularly true in an Intelligence Community institutional culture in which knowledge literally is power – in which the bureaucratic importance of an agency depends upon the supposedly 'unique' contributions to national security it can make by monopolizing control of 'its' data-stream." [65]

The Congressional inquiry into September 11th exposed dozens of examples of intelligence hoarding and excessive secrecy – a form of bureaucratic competition not for better intelligence but for status and power. The staff director of the September 11th inquiry summed up the findings in her summary statement:

> Finally, the record suggests that, prior to September 11th, the U.S. intelligence and law enforcement communities were fighting a war against terrorism largely without the benefit of what some would call their most potent weapon in that effort: an alert and committed American public. One need look no further for proof of the latter point than the heroics of the passengers on Flight 93 or the quick action of the flight attendant who identified shoe bomber Richard Reid.[66]

This fundamental point is key to the future debate over national security secrecy. The current climate is one of information phobia. But information is security and openness is our best defense. Americans, whether they want to or not, need to know when airport security is lethally porous. They need to know if and when and where we are vulnerable to biological or nuclear attack. Only when the public is fully informed about such vulnerabilities will there be sufficient pressure to move our leaders to act.

The only way we will beat thoughtless restrictions on information is to show how those restrictions actually stop us from fighting terrorism. The mantra of the moment is an old familiar one from wartime, "loose lips sink ships." Perhaps the Enron scandal will come up with a new alliteration, maybe along the lines of "off-the-books means off-the-wall." Because the first casualty of excessive secrecy is honest policy, policy the American people will support, policy that will be effective. Thinking back to the Iran-contra scandal, where secrecy hid a cabal of zealots like Oliver North doing the President's bidding against the will of Congress and his own Cabinet, maybe the rhyme would be "secret Ollies make more follies."

Only a few months before September 11th, a group of former CIA and White House officials and Cuban exiles went back to the beach at the Bay of Pigs, for a 40th anniversary autopsy on that debacle. We now know the CIA didn't even share the secret invasion plans with its own Cuba analysts, who could have told the operators there was no chance of an army uprising against Castro. Back in 1961, President Kennedy called up the publisher of *The New York Times* to try to spike that paper's pre-invasion expose, and afterwards JFK said he wished the *Times* had published everything – maybe then they'd have called off the invasion before it became "a perfect failure."67

Secrecy is the enemy of efficiency, as well. Look at Enron, now the poster child of a perfect failure, founded by a Ph.D. economist and devoted to turning everything into a market, but hiding its own debts and inflating its profits as if the rules of transparent information that make all markets work somehow didn't apply in Houston. Those same rules also apply in the war against terrorism: Just listen to the testimony before Congress from the mayors and police chiefs, including New York City mayor Rudy Giuliani himself, complaining that the big problem is the federal government does not share information with the locals.

Perhaps the single biggest success against domestic terrorism involved a major sharing of information, against the instincts of law enforcement officers, but under a threat of violence unless the information went public. This was the case of the Unabomber, the terrorist Harvard-educated Luddite who blew up scientists with letter bombs, randomly. How did the United States catch the Unabomber? After he threatened undifferentiated violence unless major newspapers published his anti-modernism manifesto, finally the FBI and the Justice Department made that recommendation to the major newspapers. *The Washington Post* printed a special section to contain the Unabomber's 35,000-word screed, and convinced *The New York Times* to swallow half the cost. Newspapers across the country circulated his crank letter file, and told the world everything we knew about him – and his brother recognized the facts and turned him in. Openness empowers citizens.[68]

The biggest U.S. success against foreign terrorism in the last ten years – that is, preventing terrorism before innocent people were killed, rather than punishing terrorists with cruise missiles – took place in Washington state, at Port Angeles, at the ferry dock from Victoria, Canada. Again, openness rather than secrecy meant security. On December 14, 1999, an alert Customs inspector named Diana Dean stopped the last car off the ferry, a large late-model Chrysler with a big trunk. The man behind the wheel was sweating in the cold, and he had driven an out-of-the-way route in order to take the ferry. So Diana Dean asked the driver to get out and open the trunk. He bolted, and Dean's co-workers caught him hiding under a car six blocks away. In the trunk were 130 pounds of fertilizer-style explosives and four homemade timers – apparently destined for Los Angeles Airport or the Seattle Space Needle for the millenium. No TOP SECRET CIA message had

come in to Diana Dean that day, warning of Ahmeds smelling of ammonia. But she had read, extensively, about the Oklahoma City bombing and the 1993 attempt on the World Trade Center – all public information based on public trials.[69]

Openness empowers citizens, weeds out the worst policy proposals, ensures the most efficient flow of information to all levels of law enforcement, makes a little more honest the despots who are our temporary allies against terrorism. Openness keeps our means more consistent with our ends. But we need to drop the idea of balancing this fundamental value against national security. To admit the notion of balancing is to lose the debate over where to balance. The appropriate attitude is the one articulated by Justice Brennan in 1980 (unfortunately, in a dissent):

> [T]he concept of military necessity is seductively broad, and has a dangerous plasticity. Because they invariably have the visage of overriding importance, there is always a temptation to invoke security 'necessities' to justify an encroachment upon civil liberties. For that reason, the military-security argument must be approached with a healthy skepticism...[70]

The government has successfully framed the debate after 9/11 as terrorism fighters versus civil libertarians, as soldiers versus reporters, as hawks versus doves. In wartime, the poundage of the former will always outweigh the latter, and the Bush administration has guaranteed wartime for the foreseeable future. So our task is to reframe the debate and leave behind the balancing act. We need to place openness where it belongs, not only at the center of our values, but also at the center of our strategy for security.

NOTES

[1] See Arnold Wolfers, "'National Security' As An Ambiguous Symbol," *Political Science Quarterly* 67 (December 1952), pp. 481-502.

[2] See the extremely useful introduction to the history of secrecy in the United States in Arvin S. Quist, *Security Classification of Information: Volume 1. Introduction, History, and Adverse Impacts* (Oak Ridge, Tennessee: Martin Marietta Energy Systems Inc., September 1989), pp. 10-24. The Quist study is available online thanks to the Federation of American Scientists' Project on Government Secrecy, at www.fas.org/sgp/library/quist/index.html

[3] Daniel P. Moynihan described this as "the unavoidable tension" in his "Appendix A: Secrecy: A Brief Account of the American Experience," in *Report of the Commission on Protecting and Reducing Government Secrecy* (Washington D.C.: Government Printing Office, 1997), S. Doc. 105-2, p. A-6.

[4] President George Washington to U.S. House of Representatives, March 1796, cited in United States v. Curtiss-Wright Export Corp., 299 U.S. 304 (1936), quoted in Stephen Dycus, Arthur L. Berney, William C. Banks, Peter Raven-Hansen, eds., *National Security Law - Third Edition* (New York: Aspen Publishers, 2002), pp. 65-66.

[5] Herbert N. Foerstel, *Freedom of Information and the Right to Know* (Westport, CT: Greenwood Press, 1999), p. 8.

[6] Nathan Miller, *Spying for America: The Hidden History of U.S. Intelligence* (New York: Dell, 1989), p. 65.

[7] See generally, Garry Wills, *Cincinnatus: George Washington and the Enlightenment* (Garden City, NY: Doubleday, 1984).

[8] Stephen Dycus, et. al., eds., *National Security Law – Third Edition*, pp. 536-538.

[9] Arvin Quist, *Security Classification of Information*, pp. 12-13. Quist also quotes Lincoln's Second Inaugural: "The progress of our arms, upon which all else chiefly depends, is as well known to the public as to myself."

[10] Arvin Quist, *Security Classification of Information*, pp. 14-18.

[11] This is one of two fundamental problems with the treatment of the issue in the critically-praised book by the late Daniel P. Moynihan, *Secrecy: The American Experience* (New Haven: Yale University Press, 1998). Moynihan misplaced his historic focus on the World War I period, and for the later period presented a polemic rather than scholarship on issues like the CIA assessment of the Soviet Union. See the critique by Steven Aftergood, "Secrets and Lies,"

Bulletin of the Atomic Scientists (March/April 1999), pp. 59-60.

[12] James Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency* (New York: Doubleday, 2001), p. 3. Bamford's introduction contrasts the 1930 vault to the 2001 "Crypto City" which occupies hundreds of acres at Fort Meade, Maryland and includes listening posts around the globe.

[13] *Schenck v. United States*, 249 U.S. 47 (1919), p. 52.

[14] *Near v. Minnesota*, 283 U.S. 697 (1931), p. 716.

[15] Grosjean v. American Press Association, 297 U.S. 233 (1936), quoted in Herbert N. Foerstel, *Freedom of Information and the Right to Know*, pp. 9-11. For Justice William Brennan's discussion of Schenck and Near in the context of the 1971 Pentagon Papers case, see Stephen Dycus, et. al., eds., *National Security Law – Third Edition*, pp. 1033-1034.

[16] Harold C. Relyea, "Historical Development of Federal Information Policy," in Charles R. McClure, et. al., eds., *United States Government Information Policies: Views and Perspectives* (Norwood, N.J.: Ablex Publishing Corporation, 1989), pp. 36-37.

[17] Enrico Fermi, "Physics at Columbia University," *Physics Today 8* (November 1955), p. 13, quoted in Robert S. Norris, *Racing for the Bomb: General Leslie R. Groves, The Manhattan Project's Indispensable Man* (South Royalton, Vermont: Steerforth Press, 2002), p. 259.

[18] Letter of June 27, 1958, quoted in Robert S. Norris, *Racing for the Bomb*, pp. 253-254.

[19] For a detailed discussion of these statutes, see Arvin Quist, *Security Classification of Information*, pp. 52-62. The "before or after" quote is on p. 53.

[20] General Leslie R. Groves in Congressional testimony, October 9, 1945, quoted in Arvin Quist, *Security Classification of Information*, p. 63. Quist refers to the Hiroshima explosion as in effect the first declassification of nuclear information.

[21] For the most authoritative treatment of this secret history, see Jeffrey T. Richelson, *The U.S. Intelligence Community – Fourth Edition* (Boulder, CO: Westview Press, 1999). For its secrecy permutations, see Kate Doyle, "The End of Secrecy: U.S. National Security and the New Openness Movement," in Craig Eisendrath, ed., *National Insecurity: U.S. Intelligence After the Cold War* (Philadelphia: Temple University Press, 2000), pp. 97-99.

[22] U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities [Church Committee], *Final Report, Book I: Foreign and Military Intelligence* (94th Congress, 2nd Session, Report No. 94-755), April 26, 1976, p. 12.

[23] See Harold C. Relyea, "The Coming of Secret Law," *Government Information Quarterly*, Vol. 5, No. 2 (1988), pp. 97-116; and for the most complete collections of declassified presidential directives on national security, together with the history of the directives system, see Jeffrey T. Richelson, ed., *Presidential Directives on National Security From Truman to Clinton* (Alexandria, VA: Chadwyck-Healey and The National Security Archive, 1994), and *Presidential Directives on National Security From Truman to Bush* (Ann Arbor, MI: ProQuest and The National Security Archive, forthcoming in 2003).

[24] The transcript from White House tapes is included in the *Statement of Information, Hearings before the Committee of the Judiciary, House of Representatives, Ninety-Third Congress, Pursuant to H. Res. 803* [proposed impeachment of Richard M. Nixon], Book VII – Part 2, "White House Surveillance Activities and Campaign Activities," (May-June 1974), pp. 874-876.

[25] For a succinct overview of executive orders on secrecy, see Harold C. Relyea, "Historical Development of Federal Information Policy," in Charles McClure, et. al., eds., *United States Government Information Policies: Views and Perspectives* (Norwood, N.J.: Ablex Publishing Corporation, 1989), especially pp. 38-43. For extensive detail on the EOs, see Arvin Quist, *Security Classification of Information*, pp. 25-43. The ALA chronology, edited in multiple editions over the years by Anne Heanue, is available from the ALA Washington Office.

[26] *New York Times Co. v. United States*, 403 U.S. 713 (1971), p. 728 (Justice Potter Stewart, concurring).

[27] See Frank Snepp, *Irreparable Harm: A Firsthand Account of How One Agent Took On the CIA in an Epic Battle Over Free Speech* (Lawrence: University Press of Kansas, 2001). Among other revelations, Snepp quotes the personal notes of Justices Thurgood Marshall and William Brennan to document what columnist Anthony Lewis called the "travesty of judicial reasoning" in the case.

[28] See Thomas S. Blanton, ed., *The Pentagon Papers: Secrets, Lies and Audiotapes* (National Security Archive Electronic Briefing Book No. 48), posted June 5, 2001; updated June 29, 2001; at www.gwu.edu/~nsarchive/NSAEBB/NSAEBB48/index.html.

[29] Erwin N. Griswold, "Secrets Not Worth Keeping: The Courts and Classified Information," *The Washington Post*, 15 February 1989, p. A25.

[30] For a summary of the case and the new evidence, see In *Re Patricia J. Herring et. al.*, "Petition for a Writ of Error Coram Nobis to Remedy Fraud Upon This Court," submitted to the U.S. Supreme Court on February 26, 2003

(awaiting docketing), by the Philadelphia law firm of Drinker Biddle & Reath. For the importance of Reynolds, see Morton H. Halperin and Daniel Hoffman, *Freedom vs. National Security: Secrecy and Surveillance* (New York: Chelsea House, 1977), pp. 103-104; and Stephen Dycus, et. al., eds., *National Security Law – Third Edition*, pp. 975-979.

[31] Stephen Dycus, et. al., eds., *National Security Law – Third Edition*, pp. 805-807.

[32] Quoted by Stephen Dycus, et. al., eds., *National Security Law – Third Edition*, p. 808 and 821.

[33] See Remarks of Daniel Metcalfe and Eric Glitzenstein in "American Bar Association Symposium on FOIA 25th Anniversary," *Government Information Quarterly*, Vol. 9, No. 3 (1992) pp. 253-4.

[34] See Harry A. Hammitt, David L. Sobel, and Mark S. Zaid, eds., *Litigation Under the Federal Open Government Laws 2002* (Washington D.C.: Electronic Privacy Information Center, 2002), pp. 35-54, and the discussion in Stephen Dycus, et. al., *National Security Law – 3rd edition*, pp. 933-943, including the D.C. Circuit's opinion in *Ray v. Turner*, 587 F.2d 1187 (1978).

[35] For the Arms Export Control Act and for the Classified Information Procedures Act, see the discussions in Stephen Dycus, et. al., eds., *National Security Law – Third Edition*, pp. 482-485 and pp. 884-888, respectively.

[36] *1997 Report of the Commission on Protecting and Reducing Government Secrecy*. The cost figures are on pp. 9-10, the page estimates are on p. 74.

[37] *1997 Report of the Commission on Protecting and Reducing Government Secrecy*. The disagreement on overclassification is on p. 36.

[38] CIA, *Task Force Report on Greater CIA Openness* (December 21, 1991).

[39] See The National Security Archive, "The CIA's El Salvador," *The New York Times*, December 17, 1993, p. A39; Kate Doyle, "The Guatemalan Military: What the U.S. Files Reveal," National Security Archive Electronic Briefing Book 32, presented in Guatemala City and posted June 1, 2000 at www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB32/index.html; and Peter Kornbluh, *The Pinochet File* (New York: The New Press, 2003 forthcoming).

[40] Warren I. Cohen, "At the State Department, Historygate," *The New York Times*, May 8, 1990, p. A29; and Kate Doyle, "The End of Secrecy: U.S. National Security and the New Openness Movement," pp. 102-104.

[41] *Final Report of the Assassination Records Review Board* (Washington D.C.: Government Printing Office, 1998, 208 pp.) provides specific recommendations for reform, as well as a withering critique of official secrecy, not only relating the Kennedy assassination, but to the general operations of the CIA and the government.

[42] Tom Blanton and Steven Aftergood, "The Wall of Secrecy Finally Cracks (A Little)," *The New York Times*, January 18, 1995, p. A21. See also the 1997 Report of the Commission on Protecting and Reducing Government Secrecy, at pp. 50-51 and 60. For a useful summary of the Clinton openness policies, see Eli J. Lake, "Clinton's Declassification Legacy Secure; Policies May Not Be," *United Press International*, November 14, 2000.

[43] Steven Aftergood and Tom Blanton, "The Securocrats' Revenge," *The Nation*, August 9/16, 1999, p. 20; Kathy Sawyer, "U.S. Masks Data on Tracks of Satellites," *The Washington Post*, April 1, 1999, p. A21..

[44] For copies of legal complaints and proceedings in the various FOIA cases brought by Steven Aftergood of the Federal of American Scientists for release of the intelligence budget, see www.fas.org/sgp/foia/victory.html, www.fas.org/sgp/foia/intel98.html, and www.fas.org/sgp/foia/1947intb.html.

[45] See David Holloway, *Stalin and the Bomb: The Soviet Union and Atomic Energy*, 1939-1956 (New Haven: Yale University Press, 1994, 464 pp.).

[46] Vice President Dick Cheney interview with Cokie Roberts, *ABC News This Week*, 27 January 2002.

[47] For LBJ's signing statement, Ford's veto statement, and copious legislative history, see Will Ferroggiaro, Sajit Gandhi, and Thomas Blanton, eds., "The U.S. Freedom of Information Act at 35," National Security Archive Electronic Briefing Book 51, at www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB51/, posted July 1, 2001.

[48] Rumsfeld quoted in Mark Tapscott, "Too Many Secrets," *The Washington Post*, November 20, 2002, p. A25.

[49] For a history of the politics of the U.S. Freedom of Information Act, see Thomas S. Blanton, "U.S. Experience with Freedom of Information Law: Congressional Activism, News Media Leadership, and Bureaucratic Politics," InterAmerican Dialogue Conference on Access to Information in the Americas, Buenos Aires, Argentina, December 12, 2002. The FBI document was obtained under FOIA by Thomas Susman, counsel to Senator Kennedy and a leading author of the 1974 amendments.

[50] The signing statement is on-line at www.fas.org/sgp/news/2002/wh102302.html, together with key documents of the Bush administration's secrecy policy and national security secrecy claims.

[51] *1997 Report of the Commission on Protecting and Reducing Government Secrecy*, p. 15.

[52] See Jesse J. Holland, "GAO to Sue White House Over Energy Task Force

Documents," *The Associated Press*, January 31, 2002, for a succinct statement of the case.

[53] For the text of the Executive Order, statements from Congressional testimony, White House statements, and the legal complaint filed by historians and public interest groups, see www.gwu.edu/~nsarchiv/news/20011128/ and www.citizen.org/litigation/briefs/FOIAGovtSec/PresRecords/index.cfm

[54] For the text of the Ashcroft memorandum, see www.usdoj.gov/foia/04foia/011012.htm. For the results of the audit, see "The Ashcroft Memo: 'Drastic Change' or 'More Thunder than Lightning?'" The National Security Archive Freedom of Information Audit, posted March 14, 2003 at www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB84/index.html.

[55] The legal case is *Center for National Security Studies et. al. v. Department of Justice*; a useful summary of the case and many related secrecy issues is Reporters' Committee for Freedom of the Press, *Homefront Confidential: How the War on Terrorism Affects Access to Information and the Public's Right to Know – Third Edition*, March 2003, at www.rcfp.org/homefrontconfidential.

[56] Dan Eggen, "On Hill, Ashcroft Defends Anti-Terror Tactics," The Washington Post, December 6, 2001; and "The Ashcroft Smear," Editorial, *The Washington Post*, December 7, 2001, p. A40.

[57] See Reporters' Committee for Freedom of the Press, *Homefront Confidential*, pp. 55-56.

[58] Bill Sammon, "Web sites told to delete data," *The Washington Times*, 21 March 2002.

[59] William J. Broad, "U.S. Selling Papers Showing How to Make Germ Weapons," *The New York Times*, January 13, 2002, p. A1.

[60] For multiple examples of censoring vulnerabilities rather than fixing them, see www.ombwatch.org/article/archive/104/.

[61] Vannevar Bush, *Science – the Endless Frontier: A Report to the President on a Program for Postwar Scientific Research* (Washington D.C.: Office of Scientific Research and Development, July 1945), quoted by Arvin Quist, *Security Classification of Information*, p. 96.

[62] R. C. Tolman, R.F. Bacher, A.H. Compton, E.O. Lawrence, J.R. Oppenheimer, F.H. Spedding, and H.C. Urey, *Report of Committee on Declassification*, Memorandum to Maj. Gen. L.R. Groves, November 17, 1945, P. 3, quoted in Arvin Quist, *Security Classification of Information*, p. 97.

[63] Edward Teller, Letter to the Editor, *The New York Times*, May 27, 1973, quoted in Stephen Dycus, et. aL., eds., National Security Law – Third Edition, p. 1047.

[64] "Lost Chance on Terrorists Cited: INS, FAA Might Have Found 2 of 19 Hijackers, Officials Say," *The Washington Post*, October 2, 2002, p. A1.

[65] Vernon Loeb, "When Hoarding Secrets Threaten National Security," *washingtonpost.com*, 26 January 2003.

[66] Eleanor Hill, Staff Director, "Joint Inquiry Staff Statement," 17 October 2002, p. 5, see www.fas.org/irp/congress/2002_hr/101702hill.html.

[67] For extensive detail on the Bay of Pigs 40th anniversary conference, see the National Security Archive website at www.gwu.edu/~nsarchiv/bayofpigs/index.html.

[68] See the September 19, 1995 special section of *The Washington Post*, and the joint statement by the publishers of the *Post* and the *Times*.

[69] For the most thorough report of the Ressam arrest, see Josh Meyer, "Border Arrest Stirs Fear of Terrorist Cells in U.S.," *Los Angeles Times*, March 11, 2001, p. A-1.

[70] *Brown v. Glines*, 444 U.S. 348, 369 (1980) (Justice William Brennan, dissenting).

NATIONAL SECURITY AND OPEN GOVERNMENT IN THE UNITED KINGDOM

John Wadham, Director, Liberty
Kavita Modi, Assistant Researcher, Liberty

INTRODUCTION

"Unnecessary secrecy in government leads to arrogance in governance and defective decision-making. The perception of excessive secrecy has become a corrosive influence in the decline of public confidence in government. Moreover, the climate of public opinion has changed: people expect much greater openness and accountability from government than they used to."

> Introduction to the White Paper on Freedom of Information, December 11 1997.

"The traditional culture of secrecy will only be broken down by giving people in the United Kingdom the legal right to know."

> Preface to the White Paper on Freedom of Information by the Prime Minister, Tony Blair, December 11 1997.

Freedom of information is of fundamental importance in increasing the democratic accountability of public bodies and the public's involvement in the democratic process. The power of the executive vis-à-vis Parliament in the United Kingdom is such that traditional safeguards are no longer enough to reign in the Government and prevent abuses of power. Further, the expansion of government in recent decades and proliferation of quangos has meant that the arm of government stretches much further than it ever has before, often through unelected and unaccountable organizations. The electorate cannot fully participate and prop-

erly exercise their voting rights if they only have sketchy information about what the present government has been doing in their name. Transparency in government also leads to higher standards within administration: if a public authority has to give reasons for a decision, this should ensure that the subject in question is given more than just cursory consideration.

Governments now hold a great deal of information about their citizens, particularly those who make a substantial use of public services. People need to make sure that information held about them is correct, particularly as this information could affect their access to public services. People also need a right of access to personal information held by public bodies because it may have an impact on an individual's life and their identity; for example, where a person has been brought up in care and does not know the circumstances of their early childhood.

Despite the bold statements quoted at the beginning of this article (which were made within months of the election of the new Labour Government), the UK Government's commitment to open government was soon substantially diluted. The Freedom of Information Act 2000 was indeed passed, but its provisions are relatively feeble compared to those proposed in the White Paper. The Government would have liked the legislation to be watered down further, but consistent pressure from parliamentary lobbyists ensured that this could not be done. Since the Act was passed, the Prime Minister has made it clear that bringing the new legislation into force is not a priority; he has rejected timetables for implementation, and postponed the implementation of the most significant right – that of access – until January 2005.[1]

As the Prime Minister has recognised, there is a culture of secrecy in the Government of the United Kingdom which is unlike that in most other democratic nations. It surpasses the level of discretion necessary to safeguard national security, or other vital interests, to become a default position, an unthinking reliance on secrecy. Lustgarten and Leigh comment that "Information about the government's activities and the basis of its decisions is thought to be, literally and metaphorically, the property of government itself, to be distributed to the wider public as and when it thinks proper or necessary."[2] These attitudes have begun to change, and the Code of Practice on Access to Government Information and the new Act have helped this development, but the lack of enthusiasm from above

is unlikely to foster an environment where changes in embedded practices and modes of thinking are properly embraced.

In addition, the government's response to the events on September 11, 2001 has made freedom of information less of a priority and national security significantly more important.

THE CURRENT FREEDOM OF INFORMATION REGIME IN THE UNITED KINGDOM AND ITS PROBLEMS

Background

Until the rights of access contained in the new Freedom of Information Act are in force, there is no legal right to obtain any kind of information or documents from central government. UK citizens are left to rely upon a Code of Practice – which encourages openness in government but does not guarantee it.

This state of affairs is blatantly inadequate, and fails to reflect the importance of freedom of information. The failures of the present system have been demonstrated time and time again by the continuous stream of government scandals and cover-ups, and security and intelligence whistleblowers. Clive Ponting leaked Ministry of Defense documents concerning the sinking of the Belgrano by British forces during the Falkland War. He revealed that the Argentinean ship had posed no threat to British forces when it was sunk, contrary to what the Government had said. He was charged under the 1911 Official Secrets Act, but was acquitted by a jury in 1985, to the great embarrassment of the Government. A few years later, the Government got itself in more hot water by its absolute refusal to allow former MI5 (the internal secret service) officer Peter Wright's book, *Spycatcher*, to be published in the United Kingdom. The revelations made in the book were not particularly damaging to the Government of the day, as they concerned an MI5 plot to discredit Prime Minister Macmillan in the 1960s. However, the Government continued to fight publication even after the book had been published abroad and was available in the UK, and had been partially serialized in the national press.

These examples show how the lack of accountability in public bodies, particularly the security and intelligence services, can lead to cover-up on a grand scale. They also show the degree of resistance in government to allow secret information to be revealed, even where disclosure is clearly in the public interest, or the information in question has already been made widely available.

In the early 1990s, the directors of the engineering firm Matrix Churchill were prosecuted for selling machine tools to Iraq which could be used to make weapons, supposedly in breach of the arms embargo. The Government tried to use Public Interest Immunity certificates to prevent the disclosure to the defendants and the court of the fact that the Government had relaxed the embargo without informing Parliament, and had known all about the Matrix Churchill transaction at the time. However, the judge refused to accept the certificates and as a result, the case collapsed, leading to a huge scandal and an independent inquiry into the affair. More recently, the Phillips Inquiry into the BSE crisis (concerning "mad cows") found that there had been a cover-up in the initial stages of the crisis, and that openness would have led to a better handling of the problem.

The new Freedom of Information Act would not necessarily have allowed access to the documents and information at the heart of these scandals. The class exemption for the security and intelligence services combined with the blanket, life-long prohibition on disclosure in the Official Secrets Act means that Peter Wright would be in the same position today despite changes in the law. In other areas, the information may fall into the scope of a qualified exemption, and disclosure would therefore depend on the public body's assessment of where the public interest lay. This situation does not inspire optimism, especially in the light of the conclusions of the Scott Report: "In circumstances where disclosure might be politically or administratively inconvenient, the balance struck by government comes down, time and time again, against full disclosure."[3]

Definition of National Security

National security has never been defined in any UK legislation.[4] Nor does the European Convention on Human Rights, which has been incorporated into UK domestic law by the Human Rights Act 1998, define this term, which is used to permit exemptions to many of the rights in

the Convention. The European Court of Human Rights has encouraged the domestic courts to take a more rigorous approach when considering government claims regarding national security, and not to be overly deferential to the executive in this area.[5] Following the adverse ruling in *The Chahal*, the Government set up the Special Immigration Appeals Commission (SIAC). In the case of *Rehman*[6], SIAC decided that it does have jurisdiction to decide the meaning of the phrase a "danger to national security," as it applies in immigration legislation. The Court of Appeal upheld this decision,[7] but disagreed with SIAC's definition of national security, which it decided was too narrow. On appeal to the House of Lords,[8] it was decided that, contrary to SIAC's ruling, the definition of national security should be wide enough to include indirect threats to the United Kingdom's national security by threats to other states and that the assessment of the threat to national security was essentially a matter for the executive rather than the courts.

These cases concerned the process by which a non-British citizen could be deported because their presence was "not conducive to the public good" for reasons of national security.[9] In fact the new "internment" (detention without trial) provisions have been grafted onto this process.[10]

Current Provisions Covering Access

Public records

The Public Records Act 1958 usually gives access to records 30 years after the last entry on the file was made, though some files are now opened earlier. The following section summarizes existing methods of gaining access to information before the period of 30 years has passed. There are various rights to specific types of information held by public bodies, or information that is available in specific circumstances.

The Data Protection Act

The Data Protection Act 1998 gives people a right of access to their own personal data that is held by public authorities and public bodies. It also gives a right to access to personal data from private bodies and corporations. The original Data Protection Act[11] only applied to computer based information and was introduced as a result of the Council of

Europe's Data Protection Convention.[12] The 1998 Act was required by the European Union's Data Protection Directive.[13] Both the Convention and the Directive included national security exemptions.

Not surprisingly, the right to subject access under the current 1998 Act is subject to national security exemptions.[14] The Act gives the minister the power to certify that the exemption applies (making it difficult, if not impossible, to challenge the factual basis of this decision in the courts). Liberty has successfully challenged the blanket ban imposed by the government preventing access by individuals to the files held on them by the Security Service.[15] Unfortunately, the government subsequently imposed a new certificate and our client Norman Baker MP was still refused sight of his file. In fact the Security Service will not even confirm or deny that he has one![16]

Other Provisions on Access

Some rights to information are very specific. For example, parties to litigation have a right to demand disclosure of information relevant to their case. Public Interest Immunity certificates can be used to prevent information relating to national security being disclosed through this avenue. Also, the Environmental Information Regulations 1992 confers a right to access to information concerning the environment. Regulation 4 provides that information affecting international relations, national defence or public security is confidential and is therefore exempt from the right of access.

Access to local government information is better than that to central government information. The Local Government (Access to Information) Act 1985 provides that the public may generally attend and receive papers for the meetings of local authorities. The Local Government Act 2000 places duties on local authorities to give notice of meetings and prior access to reports and imposes an obligation to make key decisions in open meetings. One of the most significant freedom of information rights is the rule which holds that prior to a local authority's audit by the Audit Commission, all relevant books, contracts and receipts must be available to the public for 15 days.

Reports of the National Audit Office (which audits all government departments and agencies) and the Public Accounts Committee investigations into government departments and agencies must be presented to Parliament, and the government must then issue a response. The Government can also establish a public inquiry to deal with important and controversial issues, such as the handling of the BSE crisis or the investigation into the death of Stephen Lawrence. However, the creation of public inquiries is entirely dependent on political pressure, as is the Government's response to their suggestions.

Another route to gaining information is through Parliament. Constituents can lobby their MPs to persuade them to ask a Parliamentary question on a particular issue. However questions touching on national security will not be put down by the Parliamentary authorities and government spokespeople will refuse to answer questions even when they slip through. Select Committees also play an important part in making government accountable. They can investigate a specific subject, or a Bill or White Paper, gather evidence and question ministers and civil servants. However the Home Affairs Select Committee has asked the Director General of the Security Service several times to give evidence to them but ministers have repeatedly prevented this. Lastly, the Parliamentary Ombudsmen has a duty to investigate complaints concerning government departments made by the public.

Some information leaks out through whistle-blowers. This is clearly an unreliable method for the public to gain access to information, particularly as the penalties for those who disclose secret information can be severe. There is a statute, the Public Interest Disclosure Act 1998, which gives protection for whistle-blowers raising genuine concerns of abuse, malpractice or cover-ups. However, this Act does not apply to employees of the security and intelligence agencies, even if the whistle-blower is exposing an illegal activity.

Freedom of Information Code

The most important route to information or documents held by central government is not a legal route, but the 'Open Government' initiatives. For example, access to official information has vastly improved in recent years through the provision of information on the government's website. The most significant initiative, however, has been the 1993 Code of Practice on Access to Government Information. This sets up a series of good practice guidelines that government departments should try to

comply with, although there is obviously no legal requirement to follow these procedures.

The Code encourages government departments to:

- •supply facts and analysis with major policy decisions;
- •open up internal guidelines about departments' dealings with the public;
- •supply reasons for administrative decisions;
- •provide information under the Citizens Charter about public services, what they cost, targets, performance, complaints and redress; and
- •respond to requests for information.

The final requirement clearly corresponds most closely to a right of access to information. The commitment to respond to requests for information contains exemptions for national security, law enforcement, internal discussion, policy advice and nationality and immigration but the Code maintains that even these types of information can be disclosed if the benefits of disclosure outweigh the harm to the public interest. Requests for information should be answered within 20 days. If the request is refused, the applicant herself can appeal to the relevant department in the first instance. If this is unsatisfactory, the Parliamentary Ombudsman has power to enforce the Code, but can only investigate a complaint after it has been referred to him by the an MP. The obvious weakness in this arrangement is that there is no legal force to lend weight to the Ombudsman's recommendations; however, Wadham, Griffiths and Rigby write that the majority of government departments do actually comply with the Ombudsman's suggestions.[17]

THE FREEDOM OF INFORMATION ACT 2000

General Provisions

The Freedom of Information Act 2000 (FOIA) is the most significant change to this area of the law for many years, and finally catches Britain

up, at least partially, with Canada, New Zealand, Australia, the United States and most Western European nations which already have freedom of information legislation in place. The implementation of the FOIA has been staggered. Some of it is already in force and all public bodies will be included in the publication scheme by June 2004. The right of access to information, however, will not come into force until January 2005.

The FOIA attempts to provide cheap and easy access to information held by public bodies, without any inquiry into why someone wishes to have access to particular information. However, the FOIA contains numerous exemptions, which substantially curtail its usefulness. The Information Commissioner has responsibility for enforcing the right of access and, in most cases, can overrule the decision of a public authority not to disclose. Appeals from the decision of the Information Commissioner can be made to Information Tribunal.

The FOIA introduces a rule that, prima facie, all material held by specified public authorities will be accessible. The FOIA also introduces a right of access and appeal on public records. The right of access will apply retrospectively, so that hundreds of documents from the last thirty years will immediately become available. Public bodies are trying to pre-empt the flood of requests that are expected regarding documents relating to controversial events, and will be making many documents available themselves.[18]

It should be noted however that the FOIA does not provide a route for access to personal information. Access to personal files is made available only by way of the Data Protection Act (see above). The FOIA provides access to other materials, primarily decisions, policy papers and background research. The FOIA regime applies only to public authorities and only to those public authorities listed in the Act or in subsequent orders made by ministers.

Section 1 imposes two distinct duties on public bodies. These are:

- •the duty to confirm or deny; and
- •the duty to disclose information.

This is fairly simple; unfortunately, the exemptions to these duties are rather more complicated. There are three sets of exemptions in the FOIA. Firstly, only those organisations listed in the Act or subsequently added by ministers are subject to the duties set out in the Act. The Security Service (MI5), the Secret Intelligence Service (MI6) and the Government's Communication Headquarters (GCHQ) are not listed and therefore are not subject to the Act at all.

Secondly, there are class-based exemptions, where all information falling into a particular class is exempt. One of these exemptions is information from, or relating to, certain security bodies (section 23). The bodies listed in section 23 include MI5 (which gathers intelligence on threats to national security within the United Kingdom), MI6 (which gathers intelligence on overseas threats), GCHQ (which listens in on communications) and the Special Forces (parts of the military such as the Special Air Service and the Special Boat Service).

Thirdly, there are prejudice-based exemptions. Under a prejudice-based exemption, information is only exempt where disclosure is likely to have the specified prejudicial effect (the prejudicial effect must be 'actual, real or of substance', not just speculative). National security is one of the prejudice-based exemptions. This third exemption relating to national security is designed to ensure that even if information from one of the security bodies is in the hands of another body, such as the police, it is still exempt from s.1.

So national security is protected in three ways:

- the relevant bodies are not listed as public authorities in Schedule 1 of the FOIA;
- the class-based exemption (Section 23); and
- the prejudice-based exemption (Section 24).

The FOIA exemptions are also sub-divided in another way. Some of the exemptions are absolute, and the rest can be described as qualified.[19] Absolute exemptions totally relieve the public body from the duty to communicate information, and from the duty to confirm or deny. The class-based exemption applying to certain security bodies is an absolute exemption. Qualified exemptions give an exemption on disclosure related to specific subjects but only where the public interest in non-disclosure outweighs the public interest in disclosure. Qualified exemptions may exclude the public body from the duty to communicate but will only exclude the duty to confirm or deny if, in all the circumstances of the case, the public interest in non-disclosure of even this information, outweighs that of disclosure. The prejudice-based exemption relating to national security is a qualified exemption. Therefore, for this exemption to apply, the public body must first consider whether non-disclosure is required for the purpose of safeguarding national security, and secondly, decide where the public interest lies.

If the request for information is refused on public interest grounds (a qualified exemption), there is an appeal procedure to the Information Commissioner. The Commissioner can decide whether the information falls into the exemption and can also review the public interest question. Generally the FOIA exemptions are not mandatory; a public body can volunteer information despite an exemption if it chooses to do so.

However, the Intelligence Services Act 1994 impose duties on MI5, MI6 and GCHQ not to disclose. Sections 2(2)(a) of the Intelligence Services Act provides that the Intelligence Service has a duty to ensure that no information is disclosed except so far as is necessary for the proper discharge of its functions, in the interests of national security, to prevent or detect crime or for the purpose of any criminal proceedings. Section 4(2)(a) of the same Act states that the Director of GCHQ has a duty to ensure that no information is disclosed except so far as is necessary for the proper discharge of its functions or for the purposes of any criminal proceedings.

Section 17 of the FOIA places a duty on public authorities to give reasons for non-disclosure of information, except where such a statement would itself involve disclosure of exempt information. This is an important safeguard, as it not only tries to ensure that public authorities have to consider the issue properly before refusing to give information, but also attempts to change the culture within government, so that the normal response is openness and not secrecy. It is very likely that reasons will rarely be given where national security exemptions are claimed.
Enforcement of the FOIA comes under the responsibility of the Information Commissioner: anyone who is unhappy with the way that a public authority has responded to their application can complain to the

Commissioner. If the Commissioner finds that the public body is in breach of the provisions, he can issue a notice ordering the appropriate action. If the notice is not complied with it is to be treated as if it were a contempt of court. Appeals against the Commissioner's decisions are possible in certain circumstances and can be brought in the Information Tribunal.

National Security Exemptions

The blanket exemption for certain bodies in the FOIA cannot be justified. Even if ninety-nine per cent of the information relating to those bodies would be exempt on national security grounds, it goes against the principle of transparency and open government to maintain a class-based exemption. The number of class-based exemptions is also a cause for concern. The problems are more acute where the class-based exemptions are also absolute exemptions (such as national security), as many of them are, as this excludes any consideration of the public interest.

As stated above, information or documents from the United Kingdom's security agencies is excluded from complying with s.1 in three different ways. Firstly, security agencies such as MI5 and MI6 are not listed in Schedule 1 and so the FOIA does not apply to them. Secondly, information directly or indirectly supplied by, or related to, bodies with security functions is exempt from the duty to communicate information and the duty to confirm or deny under the Act – the absolute, class-based exemption. The bodies are listed in Section 23 and include the MI5, MI6, GCHQ, the Special Forces and all the relevant tribunals. Finally, there is the qualified, prejudice-based exemption in favour of national security.

Although the bodies listed in Section 23 have no positive duties under the FOIA, the exemption is designed to exclude all information which may have been passed on from one of these organisation to a public authority. Under Section 23(2), a Minister of the Crown can issue a certificate that certain information falls into the Section 23 exemption and this certificate is to be taken as "conclusive evidence of that fact", unless the case goes to the Information Tribunal, which is entitled to take its own view. A Minister of the Crown is either a Cabinet Minister, the Attorney General, the Advocate General for Scotland or the Attorney General for Northern Ireland (Section 25(3)).

The underlying assumption is that it would not be in the public interest for any information from or relating to such bodies to be disclosed. This is a very sweeping assumption to make, and contradicts the attitude of increased, if limited, openness that has been displayed in the past few years. The fact that information relating to informants, or suspects, or possible threats and the response to such threats needs to be kept secret in order for such bodies to do an effective job of safeguarding the security of the nation is uncontentious. But it is no small leap for all such information, down to the day-to-day trivialities, to be kept secret.

Of course, mundane information may be of little use to anyone, but there are types of information that it would be in the public interest to make available. For example, particularly after September 11th, some information about the scale of the terrorist threat and how it is being handled would help the public to feel more secure and more vigilant in guarding against a particular type of threat, and would therefore assist, not harm national security. Some general information about how operations are carried out, and the role of security bodies would also help increase public trust in such bodies, increase confidence that they are performing their functions properly and that public funds are not being squandered on unnecessary bureaucracy.

At present this information is only disclosed when and if politicians choose to do so. It is used to promote the government's position and decisions to disclose are made on a political basis, not as a result of the right of citizens to that information.

The qualified, prejudice-based exemption protecting national security is contained in Section 24 of the Act. As with Section 23, a Minister of the Crown can issue a certificate which designates particular information as exempt under the section. This certificate can be challenged in the Information Tribunal, but the test that the tribunal must apply is the impossibly high standard of "Wednesbury" unreasonableness (Section 60) – that the decision to issue the certificate was so unreasonable that no reasonable Minister could have made it. This test, also called irrationality, derives from the law of judicial review[20] and has been much criticised in that context as the standard that must be proved by the applicant is so high that it is very rarely reached and serves to provide

decision-makers with immunity against review of their decisions by the courts. The application of this test therefore, does not provide much hope that the Tribunal will have significant leeway to overturn certificates; the issuing of such a certificate may operate as an almost complete bar to access to such information, even where it is unclear why the information comes under the national security exemption.

As Section 24 is a qualified exemption and not an absolute one, an applicant can ask the Information Commissioner to review whether the public body was right to maintain that the public interest in non-disclosure outweighs that in disclosure, and so apply the exemption.

THE OFFICIAL SECRETS ACT 1989

The Official Secrets Act 1989 (the OSA) was intended to be a liberalising measure. To some extent, it has improved on the previous legislation. However, many aspects of the OSA are still needlessly heavy-handed in their approach and fail to pay even lip-service to the value of openness and accountability in such an important area of government as the Security Services. The Spycatcher case discredited section 2 of 1911 Official Secrets Act and led to the passing of the Official Secrets Act 1989, which contains more specific prohibitions on disclosure than existed in the 1911 Act. The 1911 Act continues to make it a criminal offence to disclose secrets to the enemy. The new OSA identifies classes of information where there is a particular interest in confidentiality. These include security and intelligence services, defence, international relations and criminal investigations.

Section 1 of the OSA prevents all disclosures by MI5, MI6 and GCHQ officers. This is a blanket rule with no public interest defence. It is also unnecessary for the prosecution to show that any harm has resulted from the disclosure. A person who is or has been a member of the security or intelligence service, or has been notified by the Minister that he is subject to its provisions, is guilty of an offence if without lawful authority he discloses any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position or in the course of his work while the notification was in force. There is a defence if the person can show that he did not

know, and had no reason to believe that the information related to security and intelligence services but that is unlikely to provide much of a defence in most situations.

Section 1 fails to find the appropriate equilibrium between national security and open government. It has been widely criticised for its draconian approach. It goes against the values of a liberal democracy to criminalize freedom of expression when disclosure causes no significant damage to national security, or where disclosure is justified by a legitimate democratic interest in securing the accountability of public authorities. As we have stated above there is no requirement in section 1 for the prosecution to prove damage – and even proving that no damage resulted from the disclosure is no defence. The blanket nature of the rule is further apparent from the fact that disclosure is prohibited even where the material disclosed is already in the public domain!

Section 2 creates an offence where any Crown servant or government contractor makes a damaging disclosure about defence matters, without lawful authority, if he received the information in the course of his work. Section 3 creates a parallel offence where a damaging disclosure is made relating to national security or of confidential information obtained from another state or international organisation. Section 4 relates to disclosure of material about criminal intelligence or investigations, but only if the information falls in one of the two following categories. The first covers information likely to result in the commission of an offence, facilitate a detainee's escape from custody, prejudice the safety of those in custody or hamper the prevention or detection of crime or the apprehension suspects. The second category is that of information gathered from or relating to an interception of communications.

The OSA contains a general defence where the person making the disclosure proves that at the time of the offence he believed he had lawful authority to make the disclosure, and had no reasonable cause to believe otherwise. Lawful authority is also tightly defined to avoid any public interest argument.

The absence of a public interest defence to section 1 could be sufficient to violate Article 10 the European Convention (the right to freedom of expression) in certain cases. There is a public interest defence in civil

proceedings, which means that criminal liability can be imposed in a situation where it would not have been possible to get an injunction to prevent publication. Convicting people who act in the public interest could violate Article 10 because the exceptions to that right must be justified in terms of being necessary in a democratic society. Using the criminal law against those who perform a vital function in keeping a democracy healthy is clearly unnecessary.

However, the situation is not as clear-cut as it first seems, as in the United Kingdom, the House of Lords has held that section 1 is compatible with the Convention. The case of *R v Shayler*[21] concerned a former MI5 officer who had disclosed information and documents regarding illegality, drunkenness, incompetence and bureaucracy within the Security Service to the press. He claimed that he had been acting in the public interest, and that none of his disclosures had been damaging. Nonetheless, he was prosecuted under Section 1 and 4 of the OSA. Shayler argued that s.1 was incompatible with Article 10, unless a public interest defence was read into the OSA. Alternatively, he argued that he could use the defence of necessity as his actions were designed to prevent the needless death of civilians which would otherwise occur through the incompetence of MI5. The Court of Appeal found that necessity was a defence to Section 1, but that there had to be an identifiable act posing an imminent threat to an identifiable person, not merely a general risk to life as Shayler contended. The Court also found that the restriction on free speech was justifiable due to the potential damage that could be caused by any disclosure made by a official from MI5, and therefore there had been no breach of Article 10.

The House of Lords did not comment on necessity, but agreed with the Court of Appeal that the interference with freedom of expression was necessary and proportionate in the circumstances. They found that Section 1 did not contain an absolute ban on disclosure, as disclosure could be made to other public authorities, including police officers in the course of their duties (Section 7(3)(a)) and permission could also be sought for official authorization to make a disclosure. If this was refused, it was possible to seek judicial review of the refusal. These safeguards ensured that s.1 did not impose a disproportionate restriction of free speech, despite the fact that, prior to this case, no one had been aware that it was possible to make such disclosures, or to seek judicial review of a refusal to give official authorization. The case is still pending in the European Court of Human Rights, so it will be interesting to see what view they take of these issues, particularly considering that the law as the House of Lords saw it was clearly not accessible to anyone – accessibility being one of the requirements of Article 10.

Section 5 covers disclosure by third parties, but is plainly aimed at disclosures by journalists. The OSA is more liberal in its approach to third parties, who only commit an offence if they make a disclosure which is damaging and they have reasonable cause to believe that the disclosure would be damaging.

TERRORISM ACT 2000 (TA) AND THE ANTI-TERRORISM CRIME AND SECURITY ACT 2001 (ATCSA)

The UK has had draconian terrorism measures since before Liberty was set up in 1934. These measures stem from the violent conduct in Northern Ireland. The Prevention of Terrorism (Temporary Provisions) Act 1989 (the "PTA") was the latest Act in a series of similar Acts adopted by Parliament with the aim of limiting or preventing terrorism[22] in relation to Northern Ireland.[23] When, in 1974, the first such Act was introduced as a Bill to Parliament, the Secretary of State commented in relation to the powers contained in the Bill: "The powers...are draconian. In combination they are unprecedented in peacetime." [4] When the Act was re-enacted in 1984 certain of its provisions were extended so that suspects of "international terrorism"[25] would be subject to its provisions.

Liberty's concerns about terrorism measures are reflected in the fact that of the more than 7,000 people detained in Britain under the Prevention of Terrorism Act up to 1994, the vast majority have been released without charge and only a tiny fraction have ever been charged with anything remotely resembling terrorism. Almost without exception these people could have been arrested under the ordinary criminal law. To take an example, in 1992, when the activities of the IRA and others were still at their height, 160 people were arrested under the Act in Britain. Of these eight were charged with murder, conspiracy or possession of explosives, three were deported or excluded, twelve were charged with theft or fraud and eight with other minor offences. There is no evidence to suggest that the people charged could not have been

arrested under the ordinary criminal law. However all the others arrested, none of whom were convicted of any crime, were subjected to unnecessary arrest and detention.

Following a review a new Act, the Terrorism Act 2000 came into force in February 2001. This Act was a highly developed and recently revised body of counter-terrorism law and probably the most comprehensive and most draconian anti-terrorist legislation in Europe. This sits alongside an expansive body of criminal law (including offences over which our courts enjoy extra-territorial jurisdiction[26]).

However after September 11th there was more. The anti-terrorism bill -the Anti-Terrorism Crime and Security Act 2001 (ACTSA) - was published on November 12, obtained Royal Assent at 12.30 midnight on Thursday, December 13, and by December 19, eight people had been detained under its "internment" provisions.[27]

Liberty's concerns obviously included many of the "terrorism" measures in the Act but of equal concern to Liberty was the fact that there were a number of measures "smuggled" into this Bill which appeared either to have nothing to do with terrorism or the events of September 11, or were very much more wide-ranging in their remit.

This article cannot do "justice" to that Act's 129 sections and eight schedules or its predecessor with 131 sections and 16 schedules but instead picks out a couple of issues which relate to disclosure.

Section 39 of the Terrorism Act 2000 creates two offences intended to discourage and penalise disclosures which may damage the effectiveness of ongoing terrorist investigations. These are slightly reworded versions of the offences contained in Section 17(2) of the Prevention of Terrorism (Temporary Provisions) Act 1989. These offences may potentially violate Article 10 because they could stifle investigations into police actions against terrorism.

Section 39(2) applies if a person who knows or has reasonable cause to suspect that a constable is conducting or proposes to conduct a terrorist investigation, discloses to another anything which is likely to prejudice the investigation, or interferes with material which is likely to be relevant to the investigation. Section 39(4) creates an offence when a person who knows or has reasonable cause to suspect that a disclosure has been or will be made to the authorities (Sections 19-21 or Section 38B of the Terrorism Act, inserted by Section 117 of the ACTSA), discloses anything which is likely to prejudice an investigation into the official disclosure or interferes with material which is likely to be relevant to an investigation of the official disclosure.

These offences apply to everyone, not just those conducting the investigation. There is an exemption for those giving legal advice. There are also two general defences. If the defendant did not know and had no reasonable cause to suspect that his disclosure or interference was likely to affect a terrorist investigation, then he has not committed an offence. Alternatively, it is also a defence if the defendant had a reasonable excuse for making the disclosure or otherwise interfering with the investigation. There is an evidential burden on the defendant to raise the defence, but the onus then shifts to the prosecution to prove beyond reasonable doubt that the defence has not been satisfied.

Journalists and others commit offences by not disclosing to the authorities information about fundraising and money laundering connected to terrorism which comes to their attention as a result of their trade, profession, business or employment.[28]

Finally, anyone is guilty of an offence is they do not disclose information to the police "which he knows or believes might be of material assistance: (a) in preventing the commission by another person of an act of terrorism, or (b) in securing the apprehension, prosecution or conviction of another person…"[29]

All of these provisions have a significant chilling effect on the possibilities of obtaining and retaining information relating to national security.

THE LACK OF TRANSPARENCY IN THE SURVEILLANCE PROCESS : THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

In the United Kingdom, surveillance is always kept secret after it has taken place, even if there are no longer any national security concerns relating to that particular operation. In effect, this makes it impossible

for people to protect their human rights because they do not know that an interception has taken place. The Human Rights Act 1998 incorporated the European Convention on Human Rights into domestic law, and one of the rights guaranteed is the right to respect for a person's private and family life, his home and his correspondence (Article 8). Article 8 is not an absolute right; invasions of privacy by a public authority in accordance with the law are permitted for the purposes of protecting national security, preventing crime and disorder, protecting the rights and freedoms of others or protecting the economic well being of the country. However, the interference must be necessary and proportionate – the degree of interference with privacy must be as minimal as possible, and must be justified in terms of the severity of the specific purpose of the surveillance.

If a person does not know that surveillance has taken place, they cannot know whether or not an abuse of their rights has taken place, and cannot seek a remedy for any potential breach. David Feldman[30] argues that this state of affairs itself puts the United Kingdom in breach of Article 8 and Article 13 (the right to an effective remedy[31]).

However, the approach that the European Court of Human Rights (the European Court) will take to this issue is not entirely clear. On the one hand, the Court has given its approval to the German law that establishes a disclosure principle – a principle which determines that disclosure should generally take place, except where national security concerns operate to prevent disclosure.[32] But in the case of *Halford v. United Kingdom*[33], the European Court's approach to disclosure was feeble. The applicant suspected interceptions had taken place but could not find out conclusively if her phone had been tapped and the authorities refused to tell her. She went to the Interceptions of Communications Tribunal but the Tribunal merely stated there had been no unlawful interception without specifying whether this was because a warrant had been obtained for the interception, or because no interception had taken place. The European Court found no violation in regard to the tapping of her home phone because there was not enough evidence that an interception had taken place.

Lack of transparency is still an issue in relation to the new Regulation of Investigatory Powers Tribunal, set up under RIPA in order to provide a remedy for the abuse of investigatory powers. Authorisation for surveillance under RIPA in many cases can be decided by the police or public

authorities themselves – a decision of a court is not necessary. In telephone tapping cases, authorization is required but authorisation is given by ministers not courts.

Section 68(4) of RIPA provides that any decision given to the complainant shall be confined to stating whether or not the determination has been made in his favour or not; reasons for the decision are not given. Section 69(4) and section 69(2) give the Secretary of State power to make rules which enable or require the Tribunal to consider the complaint without the complainant being given full particulars of the reasons for the conduct in question and to exercise their powers in the absence of the complainant.

The system to deal with surveillance was first put in place as a result of a case in the European Court of Human Rights.[34] That system has been in place since 1985 and has never upheld a single case of unlawful surveillance. In fact, the tribunals that deal with complaints virtually never held hearings and never in public – even for anodyne legal argument. However, recently in another Liberty case, the Investigatory Powers Tribunal held for the first time that RIPA and the Human Rights Act confer additional civil rights on persons affected by an arguable unlawful exercise of those powers. This means that, in the context of surveillance, the right to privacy is a 'civil right' within Article 6 of the ECHR and as a result the determination of such claims are subject to the panoply of fair trial rights. The key right for these purposes is the right to open justice and the Tribunal sat for the first time in public on January 23rd 2003.[35]

Clearly, there is a need for covert surveillance to be covert in order to be effective. However, despite the Liberty case, the current system in the United Kingdom completely fails to recognise and balance the goals of national security and openness, and consequently leaves citizens open to abuse of their rights. It also significantly reduces the accountability of those agencies conducting covert surveillance, which almost inevitably leads to a culture where unwarranted invasions of privacy are more likely to take place.

CONCLUSION

To summarize, there is presently no right to freedom of information in

the United Kingdom, despite the numerous scandals and cover-ups regarding deception or dishonesty by Government, or illegal activities conducted by the security and intelligence services. The perception of those in Government and the civil service that secrecy is vital to the interests of the country, particularly in any matter concerning national security, has not diminished despite Open Government initiatives and the passing of the Freedom of Information Act 2000. The term national security remains undefined by statute and the the courts have recently given the executive a wide discretion on how it is to be assessed.

The existing provisions in the United Kingdom are comprised of the Public Records Act 1958, which only allows publication of documents after 30 years, the Data Protection Act 1998 and the Environmental Information Regulations 1992. All these statutes and regulations contain exemptions on the grounds of national security. Access to local government is better than that to central government. Some information is also accessible through parliament, litigation and audit reports. There is a Code of Practice on Access to Government Information, and this has been extremely useful in encouraging government departments to disclose information and change the culture of secrecy, but it does not give a legal right to information.

The Freedom of Information Act 2000, which is not yet fully in force, imposes two duties on the public authorities listed in the Act. These are the duty to confirm and deny and the duty to disclose information. However, the Act contains so many exemptions that it may prove to be something of a damp squib. Information relating to national security is exempted in three different ways, and there is no attempt to strike a balance between national security concerns and the demands of open government.

The Official Secrets Act 1989 prevents all disclosures by officers, or former officers, of MI5, MI6 and GCHQ, regardless of whether the disclosure damages national security, is in the public interest or whether the information is already publicly known. The draconian use of this blanket provision is unjustifiable, yet the Government showed no reluctance to make use of this provision last year against former MI5 officer David Shayler. The Shayler case raised the issue of whether Section 1 of the Official Secrets Act 1989 is compatible with Article 10 of the European Convention on Human Rights. The national courts have

decided that it is, but the case is set to go to the European Court in Strasbourg.

The extensive and continually expanding anti-terrorism provisions that exist in the United Kingdom raise numerous human rights issues. In relation to open government, reverse disclosure laws create a significant chill effect on journalists investigating allegations of terrorism.

The Regulation of Investigatory Powers Act 2000 does not allow a person to know whether they have been subjected to surveillance, even if disclosure of that information would cause no possible threat to national security. This may violate Articles 8 and 13 of the European Convention. The Tribunal set up under the Act is still shrouded in secrecy, despite a recent challenge by Liberty.

It is clear therefore that there is a long way to go before freedom of information becomes a reality in the United Kingdom. Unfortunately, the claim of national security remains a trump card in the hands of the executive, a card that is not subjected to any real independent assessment and little control by the courts.

NOTES

[1] Open Books, David Hencke, *The Guardian*, Saturday 21 September 2002.

[2] *In from the Cold: National Security and Parliamentary Democracy*, Laurence Lustgarten and Ian Leigh, Oxford University Press, Oxford, 1994, p221.

[3] *Report of the Inquiry into the Export of Defence Equipment and Dual-Use Goods to Iraq and Relate Prosecutions*, Rt Hon Sir Richard Scott V.C., (1996), Para. D1. 165.

[4] The UK Security Service was put on a statutory basis by the Security Service Act 1989. The 1989 Act also set out the functions of the service, from which it is possible to infer some concept of the meaning of national security:

Section 1(2) The function of the Service shall be the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.

(3)It shall also be the function of the Service to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands.

(4)It shall also be the function of the Service to act in support of the activities of police forces and other law enforcement agencies in the prevention and detection of serious crime.

[5] In *Chahal v. United Kingdom* [1997] 23 EHRR 413, the European Court found that judicial review had not provided an effective remedy to the applicant, in accordance with Article 13, because the national court had failed to properly examine the Government's claim that national security concerns operated in that case.

[6] *Secretary of State for the Home Department v Rehman* [1999] INLR 517 (Sp Imm App Comm).

[7] *Secretary of State for the Home Department v Rehman* [2000] 3 WLR 1240.

[8] *Secretary of State for the Home Department* [2001] 3 WLR 877

[9] Section 3, Immigration Act 1971 and Special Immigration Appeals Commission Act 1997.

[10] Section 23, Anti-terrorism, Crime and Security Act 2001.

[11] 1984.

[12] 1981.

[13] 95/46/EC.

[14] Section 28, the Data Protection Act 1998.

[15] *Baker v. Secretary of State for the Home Department* [2001] UKHRR 1275.

[16] We have taken new proceedings to challenge this but they have yet to be resolved.

[17] John Wadham, Jonathon Griffiths & Bethan Rigby, *Blackstone's Guide to the Freedom of Information Act 2000*, Blackstone Press, London, 2000, p33.

[18] "Open Books", David Hencke, *The Guardian*, Saturday 21 September 2002.

[19] Wadham, Griffiths and Rigby, *Blackstone's Guide to the Freedom of Information Act 2000*, p65-66.

[20] See the case of *Associated Provincial Picture Houses v Wednesbury Corporation* [1948] 1 KB 223.

[21] House of Lords [2002] 2 WLR 754; Court of Appeal [2001] 1 WLR 2206.

[22] The current definition is set out in section 20(1) of the Prevention of Terrorism Act: "the use of violence for political ends, and includes any use of violence for the purpose of putting the public or any section of the public in fear."

[23] On the 29 November 1974 Parliament passed the Prevention of Terrorism (Temporary Provisions) Act 1974 ("the 1974 Act"), the first of the series of anti-Terrorism Acts of which the Act under consideration is the latest. The 1974 Act was truly "temporary" as it contained provisions that made it lapse unless specifically renewed within 6 months. Later Acts were also called "Temporary" and have contained provision for review or lapse. Not so the Terrorism Act 2000.

[24].See H.C.Debs. Vol. 882 col. 35, 25 November 1974.

[25]. This is defined for instance in section 9(3)(b) as: "acts of terrorism ... except acts connected solely with the affairs of the United Kingdom or any part of the United Kingdom other than Northern Ireland."

[26] Including murder, offences on aircraft, torture and many others.

[27] Section 21.

[28] Section 19.

[29] Section 38B of the Terrorism Act 2000, introduced into that Act by the Anti-terrorism, Crime and Security Act 2001.

[30] David Feldman, *Civil Liberties and Human Rights in England and Wales*, Oxford University Press, Second Edition, p617.

[31] Article 13 is not incorporated into United Kingdom law by the Human Rights Act 1998, but the jurisprudence under it is persuasive in the national courts.

[32] *Klass v Republic of Germany*, (1978) 2 EHRR 214.

[33] (1997) 24 EHRR 523.

[34] *Malone v UK* (1984) 7 EHRR 14.

[35] Applications Nos IPT/01/62 and IPT/01/77 23/01/2003.

DIGITAL GOVERNMENT IN THE EUROPEAN UNION:

FREEDOM OF INFORMATION TRUMPED BY "INTERNAL SECURITY"

Deirdre Curtin, Professor of International and European Governance, Utrecht School of Governance, University of Utrecht

> *Globalization is an ambiguous process but one that cannot be rolled back...[W]e need to combine economic integration with cosmopolitan politics...Globalisation must become accountable and its fruits must be distributed more fairly.... The danger is however that exactly the opposite will happen. There is a risk that trans-national cooperation will become a means of creating fortresses, states in which both the freedom of democracy and the freedom of markets are sacrificed on the altar of private security.*
>
> Ulrich Beck, "Globalization's Chernobyl,"
> *Financial Times*, November 6, 2001

INTRODUCTION

Counter-terrorism strategies pursued after September 11, 2001 have at times undermined efforts to enhance respect for human rights. Not only have measures been taken in several parts of the world that suppress or restrict individual rights, but as highlighted by then UN High Commissioner on Human Rights, Mary Robinson, there "is increasing evidence that particular groups such as human rights defenders, migrants, asylum-seekers and refugees, religious and ethnic minorities,

political activists and the media are being specifically targeted."[1] This is true also in the context of the European Union (EU), and the effects may be exacerbated by measures taken by the EU Council of Ministers behind closed doors. The focus of this paper is limited to attacks on freedom of information in the aftermath of September 11, and in particular the effects of the counter-terrorism strategy followed by the European Union in that regard. This specific issue should however be placed and understood in its broader context of the effects of the counter-terrorism efforts on human rights in general and on certain groups in particular.

The US government, followed by other governments around the world, has striven to increase "internal security" by *inter alia* embarking on a path of secrecy unprecedented in recent years. In particular, freedom of information laws have come under attack and have been reduced or even suspended in the quest for more control over the sources of knowledge. In Canada for example, the Anti-Terrorism Act contains a (much-criticised) clause enabling the Minister of Justice to suspend the effect of Access to Information provisions.[2] In the UK, despite 25 years of campaigning for a Freedom of Information Act, Prime Minister Tony Blair suspended its enactment for a period of four years.[3]

In the United States, Attorney General John Ashcroft issued a directive to the heads of agencies to encourage those agencies to deny access more often to public records if a claim of invasion of privacy or a claim of breach of national security could be alleged.[4] The release of presidential records was moreover halted indefinitely by the assertion of executive privilege.[5] US State legislatures on the whole followed suit attacking open records and meetings laws.[6] Secrecy is in demand: it gives those in government exclusive control over certain areas of knowledge and thereby increases their power, making it more difficult for even a free press to check that power. The culture of secrecy is sometimes referred to as a virus, spreading from one part of government to another, and also transnationally, invading concerns where national internal security plays no role at all. The stakes are high: freedom of information as a fundamental (constitutional) value of democracy is sacrificed on the altar of internal security, as opportunistically interpreted.

At the level of international organizations, the Member State governments of the European Union have *inter alia* used the tragic events of September 11, as a means of adopting legislation in a highly secretive fashion which gives far-reaching powers to law enforcement agencies in the various Member States: and at the European Union level, to issue a European Arrest Warrant, freeze assets, include demonstrators in databases designed for terrorists,[7] and most recently to exchange information on individuals with the United States.[8]

At the same time the newly adopted access to information law in the EU[9] is being implemented in a restrictive fashion with wide derogations that are used to give priority to internal security concerns. It can be noted that prior to September 11, 2001 the EU, as a result of its fledgling Common Foreign and Security Policy, was already responding in a restrictive manner to the issue of classified information in this area and in particular sought to prune back the possible remit of the new (draft) freedom of information legislation as it applied to EU institutions and the public's right of access in that regard. The direct cause of this new "security" consciousness of the Council, of the EU in particular, was its evolving close relationship with NATO and the demands imposed by the latter with regard to providing the EU with access to NATO classified information. As a result, the EU limited the scope of its own access to information legislation.[10]

Further problems emerged as a result of the speed and the content of the EU's reaction to the terrorist offensive post September 11. These problems relate both to *process* (the secretive manner in which highly sensitive and far-reaching decisions are taken) and to *substance* (in particular the encroachment on civil liberties such as the freedom of expression, the freedom of movement, the freedom of assembly and the right to privacy).

Should a sophisticated international organization such as the EU, which is replacing (by means of supranational law) constitutional and legislative provisions on all kinds of fundamental issues at the national level (from constitutional rights of access to information to the laws on extradition between Member states to the laws on terrorism et cetera), adopt the lowest common denominator or a high standard of protection, given the more difficult legitimacy crisis faced by the EU than by any Member Nation State? Moreover, given the fact that the

Europeanization of a very wide range of policy areas takes place at a distance to individual citizens, and that these citizens have difficulty in understanding the incredibly complex decision-making processes and structures at the EU level, does that not make it even more necessary that information is made accessible by digital means in a very timely, user friendly and exhaustive fashion? The answers to these questions has everything to do with our vision of the nature of the democracy that we wish to construct at the European level and how it will interact with the national level.

THE DIGITAL DIMENSION OF EU GOVERNANCE: THE EVOLUTION OF A CITIZENS' RIGHT TO ACCESS EU INFORMATION

The first question is whether in the context of EU activity, citizens enjoy in terms of civil and political rights a right of access to information, including the right to receive that information digitally. The background to the question is the way in which access to information has taken shape within the EU over the course of the past eight years or so. The aftermath of the Danish "no" to the Maastricht Treaty prompted the first serious attempts to institutionalize a system of public access to EU documents which was made operational by the three main decision-making institutions in a joint Code of Conduct on the matter.[11] The institutions then made this non-binding Code operational in principle in their own specific institutional context by adopting decisions respectively based on their own internal Rules of Procedure.

At the time, this approach was said to highlight the committment of the three institutions to transparency. The issue of public access to their documents was something that they had voluntarily assumed in their internal rules but that they were under no legal obligation to do so in the absence of any explicit Treaty rules on the subject. In due course, other institutions and bodies - among them the European Parliment and the European Central Bank - have adopted similar rules to those of the three political institutions, mostly pursuant to recommendations issued by the Ombudsman in the context of inquiries into the existence of rules on public access to documents.[12] Despite a number of important limitations, the most critical ones being the exclusion of documents drawn up

by third parties and a number of widely drawn exceptions,[13] the Code of Conduct seemed to work quite well in practice.[14] In the event a request for access had been refused, citizens could either bring a case to the Court of Justice or complain to the European Ombudsman.

The role that the European Court of Justice has played, teasing out the implications of the rules adopted by the various institutions and laying down the broad parameters of their action, has been a significant one. It can very generally be said that whereas the Court adopted a role of fairly marginal scrutiny of the actions of the institutions in practice it nevertheless, in a whole series of cases tested the exact limits, successfully kept pressure on the institutions to make incremental steps in changing their culture of secrecy. Some of these pressures include a requirement to balance interests; scrutinize the documents on a case by case basis; and grant access to parts of documents. The court also applied the internal rules broadly, applying them to the Commissions "comitology" committees, and also to decision-making in the two supposedly intergovernmental fields, Common Foreign and Security Policy (CFSP) and Justice and Home Affairs (CJHA).[15]

It was only with the Treaty of Amsterdam in 1999 that access to documents was given treaty status and a provision made that the three institutions would adopt a legal instrument by co-decision (that is, jointly by The European Council and the European Parliament). This instrument set out the limits and exceptions to the principle by May 1, 2001. With minor delay and through a highly problematic and secretive procedure, a draft regulation was indeed adopted. It entered into force on December 3, 2001. To some extent it reflected the status quo and in certain respects it is more restrictive.[16] In particular, this is the case with regard to the issue of internal preparatory documents, sensitive/classified documents and the fact that it basically overrides more liberal national laws on the subject.[17]

THE EVOLVING DIGITAL PRACTICE OF THE EU INSTITUTIONS

The reaction of the institutions to the case-law of the Court in particular and to advances in information and computing technologies (ICT)

has been to introduce a more structured and pro-active approach to access to their infomation than was their initial inclination or practice. Part of the reaction was to establish a hyper-link (the Europa server) and to make a host of information available through the medium of the internet. As time went on, the approach of various institutions and bodies became more sophisticated in this new digital context. Thus, the Council in 1999 set up a digital register of its documents in a relatively accessible and user-friendly fashion. This has gradually been expanded and refined.

Both the Council and the Commission now include information on the new policy making fields of CFSP and CJHA on their internet sites and in the Register of Council documents. Article 11 of the new Regulation on Public Access to Documents states that each institution shall provide a public register, in which "references to documents shall be recorded without delay." The registers must be operational by June 3, 2002.

However, the Commission's Rules of Procedure are very half-hearted in their approach and if followed will almost certainly breach the obligation imposed by Article 11 of the new Regulation. It states that:

> the coverage of the register provided for by Article 11 of Regulation (EC) No 1049/2001 shall be extended gradually.

The European Parliament's formally adopted "Register of references" make no such limitations. However, its internal discussions indicate that there are at least four categories of documents which will never be made accessible to the public.[18]

One of the main ways that the Access to Documents Regulation adopted by the EU is surprising however is precisely the fact that it contains few explicit digital provisions other than to provide that access to the registers which will be set up by the Commission and the European Parliament (the Council already has one) will be provided electronically (Article 11, paragraph 1). In the United States, the Freedom of Information Act (FOIA) originally adopted in 1946 was adapted a few years ago to the new digital reality in an e-FOIA that is quite far-reaching in the scope of obligations placed on the public administration in terms of making their information available digitally and providing access in that way.[19] In particular it introduced an "electronic reading room" facility.

The issue of the digital information provision is also at the leading edge in countries such as the Netherlands that has known an Act to Promote Open Government (WOB) since 1978 (amended in 1993). This legislation deals with public access to information about the administration laid down in documents. An e-WOB is currently before the Dutch Parliament with the purpose of providing greater access to information on-line.

Of course, the concerns are very different and much more basic in a sense in Member States at the other end of the spectrum. The UK has just announced a four year delay on the implementation of its FOI Act, which was the subject of a twenty year campaign to get it on the statute books, and Germany which still has no federal law on access to information, although a draft is currently being debated.[20]

REFINING THE DIGITAL PRACTICE: THE ISSUE OF ACCESS TO CLASSIFIED INFORMATION RAISES THE STAKES

The Council and EP Regulation on Access to Documents in Article 9 makes special provision for a whole category of so-called "sensitive documents" which basically constitute classified documents (top secret, secret and confidential) originating from the institutions or the agencies established by them, from Member States, third countries or international organizations. The scope of the documents covered by these special rules includes public security documents, and documents relating to justice and home affairs. It even appears that documents within the scope of the "financial, monetary or economic policy" exception could conceivably be considered "sensitive documents" under the new rules. The effect of a classification as a "sensitive document" is that only certain persons can process the application for access to those documents and that reference to them can only be recorded in the register or released with the consent of the originator. This gives tremendous power to the originator of a document, who controls downgrading, and it also assumes that even the document number of a document included in a register will somehow threaten public security!

Given that originators have full control over classification, registration and release, there is no access whatsoever to such documents when authored by the Council or by third parties. This is a real problem in practice, with countries such as the United States, international organizations such as NATO, and even the Member States themselves effectively being given a veto over access to information in the EU context.[21] However, if the recent Court of Justice's judgment in the *Hautala* case is applied to the category of sensitive documents then the originator of a sensitive document could only veto access to the truly sensitive parts of the document. Access under the general EU access rules would have to be granted to the non-"sensitive" parts of a document. [22]

According to the new legislative system, the three institutions concerned (Council, Commission and European Parliament) had to adopt detailed internal rules on security rules and classifications (in their rules of procedure) which they did before Christmas 2001.[23] The most elaborate is that of the Commission which in effect clearly indicates an agenda of setting up a EU wide network of freely exchangeable "classified information" among the institutions, bodies, offices and agencies of the EU via intranet or other digital means. Moreover third states, international organizations and other bodies may also be included in this digital network and download such information provided that they operate equivalent security rules themselves. The only glint of light from the outside is the fact that references to classified information "may" be included in the digital register of its documents.

The EU has also adopted new IT information security (IT-INFOSEC) rules that entered into force on December 3, 2001. Their aim is to:

> safeguard EU information handled in communications and information systems and networks against threats to its confidentiality, integrity and availability.

This seems to be an important statement of purpose as far as digital governance by the European Commission is concerned. The rules apply to "all communications and information systems and networks" handling information classified as EU "confidential." This gives the rules broad scope the Commission has defined EU classified information as:

> any information and materials, the unauthorised disclosure of which could cause varying degrees of prejudice to EU interests, or to one or more of its Member States, irrespective of its origin.

THE ADOPTION OF SECRET LEGISLATION AND ACCESS TO INFORMATION: A CASE STUDY AFTER SEPTEMBER 11

The example of the Framework Decision on the European Arrest Warrants is a good illustration in terms of substance of just how far the Europeanization process has gone within the context of the EU. It amounts to a rewriting of national laws on extradition and removes some of the safeguards (procedural and substantive) that have traditionally applied in various national contexts. It leaves little to no discretion to Member States once adopted, although it will formally have to be implemented into national law. But this can involve virtually no parliamentary input even at that stage. According to the provisions of the Anti-Terrorism, Crime and Security Act[24] adopted by the UK Parliament, it can be implemented by Ministerial order and would not, even at the stage of national implementation, necessarily have to go before national parliament. The situation may of course be different in other Member States. Be that as it may, the provisions of the Framework Directive once adopted may well be relied upon by the law enforcement arms of the respective Member States in due course.[25]

The only legal quality the provisions of the Framework Decision will in any event not enjoy is "direct effect," and the only reason is that the framers of the Treaty of Amsterdam specifically stated this in the relevant legal article (Article 34(2)(b) of the Treaty on European Union. In other words, citizens in the various Member States will not be able to rely directly on its provisions and to enforce them in precedence to other national rules before a national court. The Court of Justice will have jurisdiction to entertain preliminary questions from national courts on questions of interpretation and validity of its provisions (Article 35(1) of the Treaty on European Union).

My focus is on the process of its adoption and the information available via internet and other sources at the time of its adoption by the Council (early December 2001). I traced through the information available via

internet on the Europa server[26] (Council[27] and Commission[28] home pages) on the draft Framework Decision on European Arrest Warrants[29] *just prior to its adoption by the Council* (that is September to November 2001). I then compared the information put before the two parliaments I was in a position to study: the Dutch parliament and the UK parliament. Finally I looked at the documents available on the Internet site of an organization of civil society, Statewatch.[30]

On September 19, 2001, the Commission put forward a draft proposal that can be found on internet via a link with Eurolex[31] under "legislation in preparation."[32] To find it one needs to know more or less the number one is looking for. A more accessible source is to be found under the link on its home page "justice and home affairs" and then onto the newly established site "Terrorism – the EU on the move"[33] where under the heading "documents" one will find the Commission's draft (COM (2001) 521).[34]

As an introduction to its new "terrorism" section, the European Commission explained that it had put forward "proposals aimed at eliminating legal loopholes in the EU that may help radicals suspected of violence escape justice." These proposals were examined by the EU Council of Ministers of Justice and Home Affairs on September 20, 2001[35] and the extraordinary European Council meeting on September 21, 2001.[36] The special Article 36 Committee of senior officials subsequently continued examination of the draft and came up with various reworked drafts during the course of the ensuing months. No reference to Council negotiations or even a link with the web page of the Council is provided under this specially constructed terrorism site of the Commission.

If one then went to the Council's web page, one found access to certain earlier drafts on the European Arrest Warrant. For example, under the activities headed "justice and home affairs,"[37] one could not track anything down, as it fell neither under the heading "future proposals for action" nor "lists of decisions adopted under JHA". One, in fact, had to know that one must go separately to the topic of "transparency" and then to the heading "access to documents / register"[38] in order to try and literally track down possible Council texts. A search in the register with the words "European Arrest Warrant" produced (at that time) a list of eight entries. This contained the Commission proposal, a Council document transferring the

Commission proposal to all delegations and six sets of draft Council texts / amendments (dating in time from September 24- October 10, October 31- November 14, and November 19 - December 4). Only the text from the Article 36 Committee to COREPER / Council of October 10, 2001 could be downloaded via the internet and it was a very initial text asking for some political guidance on some very specific issues of principle. The four substantive Council texts indicating where the Council's consideration of the Commissions proposal are indicated as "not available" on the Internet.

I then turned to the heading "agendas and timetables to meetings,"[39] exploring whether further substantive information could be gleaned as to the content of the Council's work on this particular subject. From the "timetables of meetings," it could be learned that a meeting of JHA Council was planned on December 6 and 7. Under "agendas" of meetings of the Council, on December 6, the day the scheduled meeting on JHA is to commence, the latest agenda for meetings refers to those that took place a week or more previously!

As a next step, one may turn to the heading "Article 36 Committee" to see if anything could be reconstructed from what is available there, after all this is the preparatory instance of the Council's draft decision. But the latest agendas for this important committee date back to the meeting it held on November 12 and 13, some several weeks previously . Out of curiosity one looks to see whether one might at least find the draft Council decision of October 31, but discovers only the provisional agenda and a document number, which on re-checking the Council register turns out to be the draft of October 31. So on November 12 and 13, the Article 36 committee was discussing the draft of October 31, and since then three further draft texts have been produced and distributed.

The amount of information that was available in two Member States was also limited. One discovered that on November 12, the Select Committee on the EU of the House of Lords made a Report *inter alia* on the European Arrest Warrant proposal in order to inform an early debate in the House on some of the proposed EU legislation concerned with terrorism.[40] During the course of drawing up the report, they took evidence from the relevant Government Minister and published it as is customary with evidence. The report itself and the debate in the House of Lords, reproduced in Hansard, are available on the internet.[41] The state of the negotiations are those reflected in the Belgian presidency

document of October 31, the only document available at the time that evidence was taken, and futhermre, it was provided only in French.

The Dutch Parliament is consulted as a matter of national constitutional law. On November 19, it received from the government what is known as an annotated agenda of the meeting to take place in Brussels on December 6 and 7. That agenda is also published on the Internet as an official document of the Dutch Parliament (in Dutch).[42] It included the draft arrest warrant, but referred to the version of October 31, which was supplied in Dutch and to the two later texts, one available in English and the most recent version only in French. The explicit rider was added to the annotated agenda, to the effect that in any event "it was the subject of on-going negotiations, and that the government would provide further information when it became available".

On December 5, only one day before the start of the relevant Council meeting, the Dutch Minister of Justice appeared before the relevant scrutiny committee of the Dutch parliament. At that meeting, parliament was given oral information as to the state of play in negotiations, but was not given the latest draft (December 4), as it was stated that it was not available at that time. The Dutch Parliament asked to agree to the substance of a text that was not made available to it. This despite the text of the Dutch constitutional provisions stating that it would receive such documents fifteen days in advance. In the event the Dutch parliament, along with the UK and Sweden, imposed parliamentary scrutiny reserves on the text as agreed in Council. Such reserves cannot alter the content of the Decision agreed upon in Council but must be lifted before it can enter into force.

By contrast, information was more readily available from a non-governmental organization, Statewatch. Statewatch maintained a very extensive and very easily accessible web site plus a special Observatory on the anti-terrorism measures under discussion after September 11.[43] Statewatch describes itself as "a non-profit making voluntary group founded in 1991 and comprised of lawyers, academics, journalists, researchers and community activists. Its European network of contributors is drawn from twelve countries. Statewatch encourages the publication of investigative journalism and critical research in the fields of the state, civil liberties and openness."[44] It proved easy to retrieve a text of the Proposed Framework Decision on the European Arrest Warrant,[45]

background material, and detailed commentary on the provisions of the available draft .

REFLECTIONS ON EU INFORMATION AND COMMUNICATIONS POLICY

It is not uncommon to come across statements to the effect that the technology behind ICT has occasioned a very fundamental shift in the role of government and governance.[46] ICT is responsible for a vast increase in the amount of information that is available, both in a quantitative sense and in the manner in which it renders information accessible. ICT, in principle, increases the transparency of processes and structures by generating information about the underlying productive and administrative processes through which public administration accomplishes its tasks. The Commission, in its *White Paper on Governance*, is content to adopt a congratulatory and superficial approach to its information policy (including the controversial new regulation on public access to documents) and some meagre thoughts in a separate communication on developing its communications policy.[47]

Indeed, further examination of the Report of the Working Group 2a (internal) - *Consultation and Participation of Civil Society* - as well as that of Working Group 1a -*Broadening and Enriching the Public Debate on European Matters* - reveals that the general attitude displayed within the Commission to the significance of ICT is a highly ambivalent one, confined largely to viewing it in purely instrumental terms. In other words, it tends to focus on the introduction of more online information (for example, databases providing information on civil society organizations that are active at European level or listing all consultative bodies involved in EU policy-making) rather than on reflecting on the institutional potential and dynamics of the technology in a broader (citizenship) framework.[48]

The obligation on institutions to make information available to the general public on request at the same time entails, the obligation to make known the information they have in their possession. Interested citizens must be able to know what public information the institutions possess and where and how it can be found. It is the task of the institutional actors, in the formal political process, to proactively make this informa-

tion available and in principle freely available.[49] This includes the establishment of a public register where, as a rule, documents that have been received and drawn up by a public authority (including all its preparatory instances) must be registered.

This would include documents that the public authority in question estimates initially to be "secret" or "classified" (i.e. not falling within the rules on access to documents but under one of the specific exceptions to the general rule of openness). Only in this way can public activities be opened up to the citizens (and their representatives) in such a way that they can choose the information they wish to obtain, without having to rely on public information services (the information that public authorities choose to give about their work). In June 2002, the Commission, the Council, and the European Parliament had separately instituted such registers as part of their obligations under the newly adopted regulation on access to their documents, which in large part they have done, although those of the Commission and the European Parliament have been subject to some criticism.[50]

Electronic media makes it possible to make such information widely available. [51] More and more it is considered an obligation on the part of all executive, administrative, legislative, and even judicial authorities within the EU to put on the internet extensive information about their tasks, their organization structure, their activities, the agendas for their meetings, as well as, information on the most important documents under discussion in that context.[52] If the documents are not directly made accessible via internet, then information should be included as to where those documents can be obtained. Initially, it could be said that the information placed on the web pages of the various institutions relating to documents, could already be considered as within the public domain.

THE ROLE OF THE NON-GOVERNMENTAL SECTOR

The decision by the Commission not to deal with the key issues of access to information and the linked question of the communication policies of the institutions is a major defect in the *White Paper on Governance.*[53] The decision pre-determined a fairly marginal role for "active" civil society representatives in its development of the governance agenda in the EU. But it is a rather futile exercise to attempt to pigeonhole as part of an exclusively vertical pyramid of accountability the role of the citizen and their civil society representatives in the manner that the Commission attempts to do in its *White Paper on Governance.* Rather, a re-imagined role for the civil society sector could invigorate considerably not only the institutions of representative democracy but also offset to some extent at least the reality of excessive bureaucratic domination. What is crucial however, to this perspective of introducing more spaces for deliberative democracy is that access to the debate is open and transparent and that there is no (or reduced) monopolization of influence behind closed doors. Information is often not sought by interested citizens because they are unaware of its existence.

Providing a greatly improved system of information is only to be considered a first step of a much larger project. It would serve as the basis for a system that allows widespread participation in policy-making processes through the mechanisms of interactive dialogue between the Union institutions and interested private actors. It would allow individuals to access the deliberative process as active participants rather than as mere passive receivers of messages. Moreover, it might well prove to be a unique opportunity for deliberations of citizens and interest groups beyond the traditional frontiers of the nation-state, without the burden of high entry costs for either individual citizens or public interest groups.[54] The danger of resulting information "overload" is clearly present. Already today citizens, groups, and national parliaments all experience difficulty in sifting through the information they receive and evaluating it to know what is and what is not important, and when precisely action and at what level, is required.

In this context, the role for the more specialized issue-oriented NGOs emerges as a kind of well informed "early-warning" mechanism helping to stimulate and focus public deliberations on related areas. Such "active" citizens can also have a pivotal role to play in ensuring the more widespread dissemination and filtering of information with the aim of assuring more concrete possibilities for political participation in the deliberative process itself. [55]

What could in 1996 still be termed the "quiet revolution" of NGO participation in international organizations took a different turn after Seattle in 1999. Since then, the European Council summits have rou-

tinely been accompanied by demonstrations and protests. Over time, it has become a clearer focus for anti-globalization protests, the EU being perceived as a *globalizierungsverstarker* and the links between anti-EU protests and anti-globalization protests have strengthened.[56] Such spectacular demonstrations and protests led not only to dismissive comment by a segment of the political elite (such as the statement by Tony Blair after Gothenburg, condemning "the travelling circus of anarchists"), but also amongst others. This led to greater realization of the need to take on board the sentiments of dissatisfaction being expressed bottom-up (also evidenced in referenda, such as the Irish vote on Nice) in the further construction of the EU.

Nevertheless, the temptation is to react in an overly authoritarian manner to certain post-national threats from "uncivil" society with the risk of unnecessarily radicalizing "civil" society. Thus, the normative response at the EU level to September 11, has been to equate protestors at summit meetings with terrorists, rather than ensuring that a "voice" is also given to those who seek change from the political process. What is interesting about this latter example is that it was civil society organizations themselves that successfully made an issue for debate in the (European) public sphere of the attempt to introduce a new and sweeping definition of terrorism.

The combination of immediate digital access to the relevant documents (provided by civil society itself and not by the responsible decision-makers) coupled with sophisticated analysis and an engagement with the formal political actors at the national level (national parliaments in particular) and at the European level (the Council and the European Parliament in particular; the European Economic and Social Committee (ESC) played no role at all) was a formula that resulted in real change to the normative provisions in question.[57]

As a result of engaged, albeit non-traditional political activity, citizens not only have much greater motivation to seek out information as to the performance of public administrators and formal decision-makers (either by themselves or through an association or interest group to which they belong): they are also better placed than ever to scrutinise the manner in which public administration tasks are carried out. Moreover, it follows that citizens no longer need or wish to have passive relations with the public authorities, but instead wish to play a vigorous part in defining these contacts as they see fit.[58] In other words, citizens are themselves developing their role, using the opportunities offered to them by ICT both in terms of acquiring information and maintaining virtual and horizontal relations with no traditional time and space constraints,[59] and are more willing to engage actively in issues now than in times where a more heroic view of politics prevailed.[60]

NOTES

[1] Statement by Mary Robinson, United Nations High Commissioner for Human Rights, Commission on Human Rights, 58th session, March 20, 2002.

[2] See, A. Roberts, "The Department of Secrets: The Chretien cabinet is using fears of terrorism to further restrict public access to information," *Ottawa Citizen*, October 18, 2001, page A 19.

[3] For details see the UK Campaign for Freedom of Information: http://www.cfoi.org.uk/doubleblow131101pr.html. The FOI Act itself was passed on 30 November 2000 and must be fully implemented by November 2005. An implementation timetable was announced by the Lord Chancellor in the House of Lords on 13 November, and is set out in the Government's First Annual Report on implementation published on 30 November. The timetable confirms that the right of access will not come into force until January 2005. However a provision requiring authorities to produce publication schemes describing information they publish proactively will be phased in earlier, starting with central government departments in November 2002.

[4] The text of the Ashcroft October 12 Memorandum is available at: http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm.

[5] Lucy A. Dalglish, Gregg P. Leslie., and Phillip Taylor, eds. *Homefront Confidential: How the War on Terrorism Affects Access to Information and the Public's Right to Know*. Committee for Freedom of the Press, 2002.

[6] See, Dalglish, Leslie and Taylor (2002).

[7] See, in particular, Council Framework Decision of June 13, 2002 on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision Official Journal L 190 , 18/07/2002 P. 0001 - 0020 2001) See also, EP Report on that proposal, A5-0003/2002, 9 January 2002. See also, Framework Decision on the execution in the European Union of orders freezing assets or evidence, Council 12636/01, 10 October 2001. See, Council Framework Decision of 13 June 2002 on combating terrorism

Official Journal L 164 , 22/06/2002 P. 0003 - 0007 which defines "terrorism" in such a way that many fear could still embrace protestors: see Statewatch at www.statewatch.org.

[8] See the agreement negotiated by the Director of Europol with the United States on the exchange of personal information, 15231/02 5 December 2002, www.statewatch.org

[9] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L 145/43 (31 May 2001) that entered into force on 3 December 2001.

[10] See further on this development, T. Bunyan, *Secrecy and Openness in the European Union: The Ongoing Struggle for Freedom of Information,* Chapter 6, http://www.freedominfo.org./case.htm

[11] Code of Conduct of 6 December 1993 concerning public access to Council and Commission documents, Council Decision (93/730/EC), [1993] O.J. L340/41; Council Decision (93/731/EC) of 20 December 1993, [1993] O.J. L340/43; Commission Decision (94/90/ECSC, EC, Euratom) of 8 February 1994, [1994] O.J. L46/58.

[12] See, ibid.

[13] In particular, the exception concerning the protection of the interest in the confidentiality of the institution's deliberations has been problematic.

[14] In 2001 the Council received 1,234 applications for a total of 7,950 documents. The statistics of the Council over 2001 show further a high percentage of disclosure, in respect of the Council 88% of the documents have been released for the procedure as a whole.

[15] See further, D. Curtin "Citizens' Fundamental Rights of Access to EU Information: An Evolving Digital Passepartout?," Common Market Law Review (2000) pp. 7-41.

[16] See, in general on the pre-Regulation status quo, Curtin (2000) , note 15.

[17] For critical commentary see Statewatch http://www.statewatch.org/news.

[18] See, in particular, www.statewatch.org.

[19] The e-FOIA amendments were subject to a staged implementation deadline: the last of the provisions were to be phased into US agency operations by the end of 1999.

[20] See the web-site of the Federal Ministry of Home Affairs, http://www.bmi.bund.de.

[21] See further, Statewatch home page: www.statewatch.org.

[22] See, "Council of the European Union disagrees on giving access to the public of positions taken by EU governments":www.statewatch.org/news

[23] See, specific provisions regarding access to documents in Annex III to the Council's Rules of Procedure, as amended by Council Decision of 29 November 2001, 2001/840/EC, O.J. L 313/40, 30.11.2001. The detailed rules on access to documents are laid down in an Annex to the Commission's Rules of Procedure, as amended by Commission Decision of 5 December 2001, 2001/973/EC, ECSC, Euratom, O.J. L 345/94, 29.12.2001. See EP Decision adapting its Rules of Procedure to the provisions of European Parliament and Council Regulation (EC) No 1049/2001 on public access to Parliament, Council and Commission documents, 13 November 2001 (Rule 172 and Annex VII) and EP Bureau Decision of 28 November 2001 on public access to European Parliament documents, O.J. C 374/1, 29.12.2001.

[24] http://www.statewatch.org.

[25] See further on this point D. Curtin and Dekker, "The Constitutional Structure of the European Union: Some Reflections on Vertical Unity-in-Diversity," in: P. Beaumont , C. Lyons and N. Walker (eds.), *Convergence and Divergence in European Public Law*, (Hart , 2002).

[26] http://europa.eu.int.

[27] http://ue.eu.int/en/summ.htm.

[28] http://europa.eu.int/comm/index_en.htm.

[29] http://europa.eu.int/eur-lex/en/com/pdf/2001/en_501PC0522.pdf.

[30] http://www.statewatch.org.

[31] http://europa.eu.int/eur-lex/en/index.html.

[32] http://europa.eu.int/eur-lex/en/search/search_lip.html.

[33] http://europa.eu.int/comm/justice_home/news/terrorism/index_en.htm.

[34] http://europa.eu.int/comm/justice_home/unit/terrorism/terrorism_sg_en.pdf.

[35] http://europa.eu.int/comm/justice_home/news/terrorism/documents/concl_council_20sep_en.pdf.

[36] http://europa.eu.int/comm/justice_home/news/terrorism/documents/concl_council_21sep_en.pdf.

[37] http://ue.eu.int/jai/default.asp?lang=en.

[38] http://register.consilium.eu.int/utfregister/frames/introshfsEN.htm.

[39] http://ue.eu.int/cal/en/index.htm.

[40]http://www.parliament.the-stationery-office.co.uk/pa/ld200102/ldselect/ldeucom/34/3402.htm.

[41] http://www.parliament.the-stationery-office.co.uk/pa/ld/ldhansrd.htm.

[42] http://www.parlement.nl.

[43] http://www.statewatch.org/observatory2.htm.

[44] http://www.statewatch.org/about.htm.

[45] http://www.statewatch.org/news/2001/sep/euarrest2.pdf

[46] ICT and Government Committee, *Citizen and Government in the Information Society. The Need for Institutional Innovation*. (Den Haag, September 2001), http://www.minbzk.nl/international/documents/pub3092.htm.

[47] European Commission: Communication on a New Framework for Co-operation on the Information and Communication Policy of the European Union, COM (2001) 354, 27 June 2001.

[48] Bovens (2001).

[49] The role of commercial publishers in this regard must clearly also be considered but here it is a matter more of a supplemental role where such publishers charge commercial rates for information to which some clear added value in terms of information provision is present.

[50] See further, www.statewatch.org

[51] Of course the assumption cannot be made that individual citizens interested in participating in this fashion all necessarily have access to the requisite hardware in order to have voice in this fashion. Clearly the provision of easy access to the computer hardware in public areas such as libraries, community halls and even public kiosks (Portugal and the Netherlands) need to be stimulated at national and local level, possibly with some EC funding.

[52] See the practice of the Europa server in that regard: http://www.europa.eu.int.

[53] see, http://www.europa.eu.int/comm/governance/white_paper/index_en.htm

[54] See too, Weiler et al. (1996).

[55] See further, D. Curtin, “Non-Governmental Representation v. Civil Society Deliberation: A Contemporary Governance Dilemma”, paper presented to ARENA Annual Conference, Oslo, 2-3 March 2002.

[56] See too, Wolf (2001) 113.

[57] See for details the Observatory on Terrorism and the Protection of Civil Liberties on the Statewatch home-page, www.statewatch.org.

[58] ICT and Government Committee, *Citizen and Government in the Information Society. The Need for Institutional Innovation*. (Den Haag, September 2001) http://www.minbzk.nl/international/documents/pub3092.htm.

[59] See further, Scientific Council for Government Policy, *Governments Losing Ground. An Exploration of Administrative Consequences of ICT* (Den Haag 1998).

[60] See, on the role of ICT in strengthening the possibilities for civil society organizations to participate in the process, Internet and Public Administration (Internet en Openbaar Bestuur), *De Schaduw Democratie* (2001), http://www.internetenopenbaarbestuur.nl/.

NATIONAL SECURITY AND THE RIGHT TO INFORMATION IN BULGARIA

Alexander Kashumov
Coordinator of Legal Projects
Access to Information Programme Foundation

In 1989, political changes in Bulgaria guaranteed the freedom of information.[1] The right to access government-held information is enshrined in Article 41 of the Constitution, in the chapter devoted to human rights. This right was born out of public concern about environmental pollution problems, as well as former state security services files.[2] In addition, political debates that were a natural result of the revived system of pluralism raised the public's interest in the work and behavior of public officials and politicians. The media began investigating public figures and provided a forum for debate.[3] Non-governmental organizations also started to be active information seekers, especially in the field of environmental protection; the Environment Protection Act (EPA) contained a chapter on access to information. Between 1997 and 1999, the Bulgarian media's interest in getting more information from government agencies gradually increased. After the Access to Public Information Act (APIA) was adopted, the media, NGOs, and citizens felt encouraged to seek information from the state and did so more often each year.[4]

At the same time, the country continues a serious practice of secrecy. Internal regulations on secrecy, unknown to the public, remained suspended, but not repelled; far from public eye, but not thrown away. Although the National Assembly in 1990 adopted a list of categories of

information that constitute state secrets that relate to national security, the government continued to hold pieces of information in secret under the old regulations.[5]

So-called "official secrets" are another type of secrets. Traditionally, their scope is defined less precisely; this category has not been précised much even now. The usually protected interests are not expressly identified in the laws and secondary legislation that govern official secrets. This exemption from the right to access information appears to be a very serious obstacle to transparency, since it is never foreseeable which of the pieces of information handled every day could be considered an "official secret."

The new regulations on both Freedom of Information (FOI) and secrecy matters apparently follow a trend for a government that is more open and accountable to citizens, which necessarily involves reconsidering what is protected information. This is the first time a statute has regulated national security exemptions. Despite this positive approach, some problems have surfaced on the legislative level. The quality of the 2000 FOI law is deficient, because its drafters lacked the knowledge or political will to meet high standards of openness. Similar problems appeared in the Protection of Classified Information Act (PCIA), adopted in 1998, because the scope of secrets was not defined with sufficient precision.[6] Its drafters' enthusiasm stemmed from their ambition to fulfill NATO requirements, rather than from a will to stick to openness standards.[7]

The lack of harmonization of the two laws is problematic on a practical level. Insufficient training, financial support, and administrative preparation impede the implementation of the FOI law,[8] while the newly established PCIA Commission is reportedly pushing agencies to comply with its classification requirements.[9]

The energy with which laws on the protection of classified information are being implemented is explained partly by the fact that there exists a body responsible for implementing them, and partly by Bulgaria's application for NATO membership. Regarding implementation of the APIA, on the other hand, the government relies on the fact that the law is passed already. The European Commission does not address the issue as an important one in its regular reports.[10]

The role of NATO requirements, and their relation to the ways in which classification laws in Bulgaria and Romania may undermine earlier openness legislation, is not clear enough.[11] Some of the new legal standards, such as time limits on document classification, probably reflect NATO requirements. Similarly, the harm test was first introduced in Bulgaria with the law on protection of classified information.[12] It is beyond doubt, however, that governments in Bulgaria and Romania [13] used the opportunity to achieve illegitimate goals as well.[14]

FREEDOM OF INFORMATION REGULATION IN BULGARIA

Constitutional Guarantee

The 1990 Constitution guaranteed, among other rights, the citizens' right to access government-held information.[15] The provision evidently was passed with the purpose of meeting public demand for more information from government authorities about their current and past activities. However, the Socialist Party that dominated Parliament, and which succeeded the Communist party that had ruled during the socialist regime, was not keen to grant much liberty in that right, as it would expose the party's past to the public. That reluctance is evident in the wording of the Constitutional provision (Art. 41, Par. 2), which reads as follows:

> Citizens shall have the right to information from state organs and establishments on questions of legitimate interest to them, when it is not a state or other secret prescribed by law or does not affect the rights of others.

This legal provision has three problems. First, it establishes a right that is dependent on a person's specific legal interest, which violates the standard of Principle III of Recommendation (81)19 of the Committee of Ministers of the Council of Europe — the statement of European standards on openness at the time. Principle III holds that access to information cannot be refused because the person requesting the information does not have a specific interest in the matter. Second, the constitutional

right is granted to citizens, not to everyone. Third, protected interests are not explicitly listed, which creates the possibility that their number will grow.

In 1996, the President asked the Constitutional Court to deliver its binding interpretation of the provisions of Articles 39 through 41 of the Constitution, which are related to freedom of expression and information and media freedoms. In its judgment,[16] the Constitutional Court stated that all of the rights contained in these provisions should be viewed and interpreted as a whole. It also held that the rights enshrined in these provisions should be considered as principles, from which the restrictions on these rights are exceptions. According to the Constitutional Court, it follows from this premise that the restrictions should be understood narrowly and applied only to protect a conflicting right or legal interest, as the constitutional provision of Article 41, Paragraph 1 explicitly prescribes:

> Everyone shall have the right to seek, receive and impart information. This right shall not be exercised to the detriment of the rights and reputation of others, or to the detriment of national security, public order, public health and morality.

The Constitutional Court held that state authorities are obliged to guarantee everyone the right to seek information as enshrined in this provision by both active disclosure and provision of access to information sources. The state's obligations should be determined by law. Consequently, the Constitutional Court found in Article 41, Paragraph 1 of the Constitution the legal ground of the right to access government-held information. The provision's wording is similar to that of Article 19 of the International Covenant on Civil and Political Rights.

This Constitutional Court's approach was of essential importance, because it interpreted the right to access information broadly, avoiding potential problems with legitimate interest as a precondition to exercise the right, the scope of people entitled to the right, and the potentially broad range of interests protected by exceptions.

Laws before FOIA

The constitutional guarantee turned out to be insufficient to ensure

effective enforcement of the right to access information. Courts took the position that without a law, they have no capacity to consider disputes over alleged violations of the constitutional right.[17] From 1997 to 2000, the Access to Information Programme (AIP) used different pieces of legislation, mainly parts of administrative laws, to argue before authorities that citizens and the media have a right to information. A general obligation to provide information (although not clearly specified) was derived from the law on recommendations, warnings, complaints, and requests (1980). Another regulation, a state council decree[18] on administrative and legal service for the population (1985), outlined some obligations to provide information to people showing a legitimate interest. Other pieces of law in different spheres also were used, such as the law on protection of the environment (1991);[19] the law on local self-government and local administration (1991); and the law on securities, stock exchanges, and investment companies (1998).

Law on Freedom of Information

Freedom of information law in Bulgaria was passed as part of a broader program of administrative reform, as in other countries in transition in the region.[20] Beyond the FOIA, administrative reform included the Law on State Administration (1998), the Law on Government Servants (1999), the Law on Public Procurements (1998), and the Law on Normative Acts (which has not been passed). The government introduced these pieces of legislation in response to the need for effectiveness and transparency in the public sector. However, while preparing the FOI draft law, it became clear that the government was unaware of the standards underlying the people's right to access public information.[21]

The administrative reform came after the huge economic and financial crisis in late 1999 and early 1997. Instability and corruption, which lead to that crisis, were accompanied by the Cabinet's refusal to service loans from outside financial institutions. When the right-wing party Union of Democratic Forces (UDF) took the majority in Parliament and appointed its government in April 1997, there was a serious expectation for openness from both the public and the two international financial institutions – the International Monetary Fund and World Bank – that signed new agreements with the government in 1997. In addition, the electorate expected that state security services files would finally be

opened, as this was the first time the UDF controlled a majority of the Parliament.[22]

Alongside these events, the Access to Information Programme (AIP) started its active work in the spring of 1997.[23] After several months of consultation on FOI cases,[24] it became clear that an FOI law was needed. The AIP's campaign to adopt such a law started at the same time as the government's work on the FOI draft. The AIP became a leader of the campaign for better legislation on access to public information. The campaign started in 1998 and continued until the law was adopted in the summer of 2000, producing a number of papers and comments by different organizations and groups[25] that were presented in several seminars and conferences, some of them including international participants.

While analyzing the proposed Bulgarian legislation, AIP lawyers noticed that traditionally, secrets are not related to the protection of a specific interest, but only to categories of information, which often are broadly defined. Subsequently, when the administration decides whether to grant an information request, it does not undertake steps to identify the protected interest or to balance interests. This explains why in most FOI cases, the Bulgarian state administration finds it is sufficient only to identify the relevant legal provision and to refer to it as a basis for denial. It does not apply the "three-part test," which requires that information relate to a legitimate aim listed in the law; that disclosure must threaten to cause substantial harm to that aim; and that the harm of the aim be greater than the public interest in releasing the information.

Parliament adopted the Access to Public Information Act (APIA) in June 2000[26] after a public debate in which the AIP played a key role. The AIP submitted a number of comments and recommendations on the different stages of the decision-making process. Representatives of the organization were present at all debates in the Parliamentary Legal Committee. Many of their recommendations were not taken into account, and others were accepted.[27]

The APIA does not meet some standards and also lacks enough clarity about how public officials should implement it. Public information is defined as information that enables citizens to form opinions about the activities of the agencies governed by the law.[28] Archival information is

excluded from the scope of the act. The right is directed to information rather than to documents.[29] Whether to review or to obtain copies of documents is the requester's preference, except in narrowly described cases. Everyone has the right to access public information, regardless of their citizenship or residence. The obligation to disclose information actively or by request is imposed on all the three branches of government.[30] Other obligated entities are those that receive state money and the so-called public law entities.[31]

The law prescribes restrictions on the right to access public information.[32] However, it does not make a clear linkage between its restrictions and the protected interests the Constitution lists.[33] The law mentions four exemptions:

(1) state secrets;

(2) office secrets;

(3) protection of third-party interest, which embraces personal data protection and business secrets; and

(4) pre-decisional opinions and recommendations.[34]

Until the Classified Information Act came in force in May 2002, there was no time limit for the exemptions.[35] Fees for providing information may not exceed the printing expense or other similar costs. Refusals to provide information are subject to administrative court review, which has two stages. No ombudsman or information commissioner was provided under the law, which appears to be a serious deficiency.

The main critical comments of AIP, the Bulgarian Helsinki Committee, and the non-governmental organization ARTICLE 19 when the bill was introduced in Parliament concentrated on the following points:

•The definition of public information is complicated and could be interpreted in a restrictive way.

•The media should not be counted among the units obliged under the law, whereas companies providing public utilities should be included.

•Exemptions from the right should be regulated precisely by pro-

viding an exhaustive list of protected interests and by setting forth the "three-part test" applicable to restrictions.

AIP paid much attention to the problem of regulating exemptions. It suggested new provisions for regulation, but the UDF Member of Parliament who introduced them in the Parliament withdrew the suggestions.[36] The next attempt in the legal committee to improve the draft also met strong opposition and failed.[37]

Today, nearly three years after these events, concern about the definition of exemptions has been proven to be realistic and warranted. The lack of strict standards for all exemptions led to an administrative practice of denying access to information simply by referring to the corresponding legal provision, without any efforts to identify the protected interest, conduct a harm test, and consider interests served by disclosure. Also, the fact that exemptions are listed in the law as "secrets" – and not as means to protect specific interests – fits comfortably with the old model of secrecy. Typical for that model is to cover a broad scope of matters with darkness without giving any key to answer the question of why access to that information is restricted.

Lack of Good Administrative Practices

Bulgarian administration needs to take some steps toward the practice of good service to citizens. Civil servants have not changed enough from being officers who only fulfill orders "from superiors" to being servants of the people. Despite the changes in legislation regulating public administration, some old schemes still exist. For example, the term in use is "governmental" instead of "civil" servant. Citizens are not guaranteed protection against abuse by public administration, because the very important Law on Administrative Procedures (1979) has not been changed much. As a result, appeals against administrative actions or omissions are not effective. There are no effective instruments other than political pressure to push public administration to act when it does not like to, because of slow court procedures and a very complicated system of compensation.[38]

All of these problems are reflected in the administration's reaction to the implementation of FOI law. The AIP's 2002 sociological survey on that issue[39] shows that the government has not undertaken necessary steps to ensure implementation of the law. In many units within the executive branch, there are no servants appointed to deal with information requests (33.7 percent of those surveyed) or places where information requests can be registered (nearly 25 percent). At the same time, AIP interviewers met negative attitudes in a number of institutions and heard expressions such as, "I do not care about YOUR law! Leave me alone!"[40]

Public administration's negligence also is evident in the cases the AIP has recorded. The number of cases in which there is no response to information requests (so-called tacit denials) continues to be large. Soon after APIA was adopted, courts refused to admit their competence to judge on such cases.[41] After vigorous arguments, in two cases in 2001 five member panels of the Supreme administrative court decided that judicial review extends to tacit denials and established court practice on that.[42] Subsequently, cases moved to the issue of declaring tacit denials always unlawful.[43]

These problems with public administration reflect on the effective implementation of FOI law and hence on the public's ability to exercise its right to access public information. They also are an obstacle to concentrating on how to apply FOI exemptions. If the ideal is that openness is a behavior, not a decision taking process, the problem in Bulgaria (and perhaps in other countries with the same background) is that still it is not even a decision taking process.

THE REGULATION OF SECRECY IN BULGARIA

Regulation of secrecy took different forms across three different time periods in Bulgaria. The first is the period of socialist times, the second is the period between late 1989 and 2002, and the third is after the Protection of Classified Information Act was passed in 2002. The first period was considered to be one of ideological war against enemies of communist regimes.[44] During the second period, the political system changed, and the principles of rule of law and human rights protection were established. Legal regulations also changed somewhat, and public attitudes viewed secrecy as a relic of the past. The

third period could be described as a time that set forth both more precise regulation on secrecy and some revival of the government's endeavor to resort to secrecy.

The Regulation of Secrecy before 1990

What documents could be classified as state secrets before 1990, as well as who could classify them and how, is not known even now, thirteen years after the changes. There was no legal instrument apart from internal rules to regulate these matters. The only legal provision that sheds some light on this is Article 104 of the Penal Code (1968), related to the crime of espionage. According to paragraph 3 of that article, "state secret" is defined as:

> facts, information and matters of military, political, economic or other character, the disclosure of which to a foreign government could harm the interests of the state and especially its safety.45

The Cabinet approved a list of "facts, information, and matters," but the list was not published.[46] According to Bulgaria's Supreme Court (1980), only the categories of data in the list which the Cabinet had approved were state secrets. The Court also held that information published in the press could not be considered a state secret anymore. Court practice in that time was far from democratic; in a 1978 case, the Court decided that the question of harm (related to national economy) was not a question to be investigated, because criminal responsibility was justified by the communication of information that was listed as a state secret.[47]

The Penal Code provides penalties for disclosure of an official secret (Article 284), an economic secret (Article 224), or other secrets (Article 360). It is notable that official and economic secrets are not defined anywhere in the law or other legislation. Communication of an economic secret is penalized if it would cause substantial harm to the economy, and communication of an official secret is subject to sanction if it would cause harm to the state or to a firm, organization, or private individual. "Secrets" under Article 360 differs from the former categories since it encompasses information of military, economic, or other character about which communication is forbidden by law, order, or another administrative document. It is important to

emphasize that all of these provisions still exist, though they are not applied. This is a threat that should not be underestimated when assessing reasons for the poor application of FOI law.[48]

The List of State Secrets

In 1990 the Parliament adopted a list of facts, information, and matters that constitute state secrets. It included three groups of data, related to defense (sixteen categories), foreign relations and internal security (five categories), and the economy (six categories, one of which was abolished in 1999). In 2000, a fourth group of data, related to aircraft safety, was added.

Not withstanding the clear scope the list set forth, executive-branch institutions continued to apply their own "standards" without minding the inconsistency. For example, on Feb. 24, 1994, the Ministry of Foreign Affairs approved a list of "facts, information, and matters" that constitute state secrets for the Ministry, and it defers considerably from those contained in the Parliament's list.

There were three levels of classification at that time, according to a regulation passed by the government: top secret of particular importance, top secret, and secret. However, there was no considerable difference between them as there was no limit on the duration of classification following socialist times. Declassification was not regulated at all.

Documents were practically declassified by order of the relevant minister or the Cabinet a few times between 1997 and 2001. The Parliament also decided in October 1994 that information about the organization, methods, and means for the performance of special assignments by the former state security services, as well as the information from agents collected by them before Oct. 13, 1991, are not state secrets under the list adopted by Parliament.

The List of Strategic Entities (State Organs and Organizations) of Significance to National Security

A government regulation from 1994[49] regulated the functions of the

National Security Service (NSS), a department in the Ministry of interior, in relation to the protection of strategic objects[50] and activities of significance to national security and of state secrets. According to that regulation, the protection had two aspects: physical protection and informational protection.

There was no definition in the regulation or elsewhere in the legislation of a strategic object of significance to national security, but the regulation provisioned that the Cabinet (that is, the Council of Ministers) should determine these objects under a request of the correspondent minister. It is seen in the regulation that the term "object" is closely related to the term "strategic state organs and organizations" (strategic entities). [51] Article 4, Par.1 of the regulation provided that the Cabinet approves and amends the list of strategic state organs and organizations.

The cabinet has never made the list public. A number of companies, even private, were registered in the list alongside state authorities.[52] The list was published briefly in the State Gazette in early 1994, [53] but in December, the newly elected socialist party government cocooned it in silence again.[54] The AIP debated the issue[55] and then published the list.[56] Despite the AIP's action, no government published the list.

At the time, Bulgarian legislation did not define the term "national security" or "strategic places and activities." The government would decide on a case-by-case basis, without taking legal requirements into consideration, whether it was necessary to put a given state agency or organization on the list. Formerly state-owned businesses, registered in the early 1990s as commercial companies with the government being the sole shareholder, evidently continued to receive special care after the Cold War.

The Cabinet's decision to list a new entity could not be challenged in the courts, because according to the Constitution, the courts are entitled to review government acts only with respect to their legality, but there was not any legal criteria for enlisting an entity as strategic. Futhermore, even if judicial review was admissible it would be impossible to find anybody with a legitimate interest to sue, since there was no FOIA in 1997 and in addition the constituitional right of everyone to access government held information was not yet enforced by the courts.[57]

The classification and safeguarding of documents was entrusted to a unit established in each authority or entity on the list. An officer from the National Security Service (NSS) worked in each unit, and the NSS exercised overall control of classification procedures.

An example of how the list worked is the inclusion of the National Electric Company (NEC) in May 1997. At that time, the Bulgarian press reported that NEC was listed among the "state organs and organizations" within which units were established to protect the facts, information, and objects that were state secrets.[58] That is how AIP was informed of the existence of the list and undertook setps to obtain a copy of it.

Bulgaria had just surpassed a huge economic crisis and hyperinflation in January 1997, followed by the resignation of the Socialist party government on February 4 and elections in April, in which the right-wing party, the Union of Democratic Forces, took the majority in the Parliament and appointed a new government. There also was serious tension about who would control the gas-flow pipes in Bulgaria.[59]

NEC was listed upon its request addressed to the Council of Ministers. In the letter, the company director said that the listing was needed as a step toward:

> solving particular issues of production security and the security of energy distribution as well as issues of limiting access to the energy-production units, energy supplies, information of cases of bad management, property damages, thefts and misuse of materials and finally securing the secrecy of classified documents.

The Protection of Classified Information Act

The 2002 Protection of Classified Information Act (PCIA) was the first statute in Bulgaria regulating all matters related to state and official secrets. It was drafted in 2000[60] and passed in April 2002. The governments referred to the necessity to draft this law as a "strategic priority."[61] It was justified by the lack of overall and statutory legislation on the matter, together with the large discretion to classify documents.

The AIP received an official invitation to participate in the discussion on the law after the NGO filed a request for access to the draft version. The draft was discussed with a working group, which was led by the National Security Service and included representatives from the Ministry of Defense, the Ministry of Interior, the Ministry of Foreign Affairs, the Ministry of Transport and Communications, and others. In April 2001, the AIP delivered its comments. It noted that a register of the classified documents should be created and made public, because citizens have no other means of watching the terms for classification, and also suggested that the definition of "state secret" should meet the "three-part test." In its comments and statements in October 2001 and March 2002, the AIP also criticized the regulation of official secrets and the lack of provisions on classification of segregable portions of documents and on deletion of documents. Accent was put on the fact that under the draft law, information falling under the definitions of state and official secrets is considered classified itself, without implementation of any procedural rules and marking. Clear classification authority was also missing.

The AIP's position was announced publicly in a discussion in the National Assembly and through the media. Two drafts with similar provisions were introduced by the UDF parliamentary group and the government. Soon before voting on the bill, the Cabinet amended it with a provision abolishing the law on access to former state security services files. After an intensive parliamentary debate, during which the UDF proposed its amendments and consulted with the AIP, the Parliament adopted the government bill in April 2002.

The next month, a group of Members of Parliament addressed the Constitutional Court with a claim that some provisions of the newly adopted law are contrary to the Constitution. They claimed that the lack of publicity for the register[62] of classified documents and the abolition of the law on access to former state security files were unconstitutional. However, they did not dispute the requirement to classify files or volumes of documents when they contain an individual document subject to classification.[63] In Decision No. 11 of 2002, the Constitutional Court held that the challenged provisions are not unconstitutional. As a consequence, the regulation, which the government passed for the application of the law, stated that the register of classified documents is classified itself.[64]

The PCIA was published on April 30, 2002. Thus the legislature fulfilled its constitutional obligation under Article 41, paragraph 1 of the Constitution, as interpreted by the Constitutional Court in its Decision No. 7 of 1996 on Constitutional Case No. 1 of 1996.[65] At the same time, however, the act was adopted as a necessary step in the application process for NATO membership, which led to some concerns – namely, that this circumstance could be used as an opportunity to restrict citizens' rights to access information. These concerns proved to be justified.

Positive aspects

Some of the act's significant achievements should be emphasized. "State secret" was defined as information that falls within the categories listed in an annex to the act, which if disclosed would harm or threaten to harm the interests of national security, defense, foreign policy, or the protection of the constitutionally established order.[66]

"Official secret" was defined in a similar way, although the protected interests are less clear. The categories of such information should be listed in a law and defined by secondary legislation. The requirement that protection should be limited to information that would be harmful if disclosed is applied to official secrets as well; however, the interests that may be considered when determining likely harm are not precisely determined.

The law also specifies the length of time information in each category remains classified. There are three levels of state secrets: top secret (30 years), secret (15 years), and confidential (five years). The duration of classification of an official secret is two years.

While the only authorities that previously exercised control over classification and related matters were security services, the newly established commission appears a step ahead.

Negative aspects

The definition of "state secret" encompasses the following protected interests: national security, defense, foreign affairs, and protection of the constitutional order. While the last interest is unclear and stems from the old system, in which the "enemy" was sought within the society, the

fact that the first three are mentioned separately also is of concern. What are considered national security issues, besides national defense and foreign affairs?[67]

The definition of national security is too broad and unclear. According to the supplementary provisions of PCIA Para.1, Item 13, "national security" means:

> a state of society and country where the fundamental human and citizens' rights and freedoms, territorial integrity, independence and sovereignty are protected and democratic functioning of the state and civic institutions is guaranteed, which results the nation saving and enlarging the wealth and in the development of the nation.

It turns out that almost everything is related to national security and therefore is subject to special treatment.[68]

Some information categories listed in the act's annex are not related to the protected interests. For example, the group of economic data usually is not linked to national security or constitutional order. In addition, the interests the "official secret" exemption protects are very broad: that is, interests of the state, and any other interest protected by law.

The law also fails to grant clear classification authority. Classification is entrusted to everyone who is authorized to sign the relevant document, which increases the potential number of classified documents.[69] People may classify information more often, either because they fear they will be sanctioned if they fail to do so, or to allow the taking of a decision far from "unauthorized" eyes. Promises that security services will practically control that process do not seem persuasive.[70]

According to the law, when a classified document is kept in a file (that is, a volume of documents), the entire file should be classified. If there is more than one classified document in the file, the classification level applied to the file will be that of the document in the highest classification level. Evidently, these provisions violate the principle that information may be classified only when its disclosure could harm protected interests.

Changes of the duration of classification of a document are not subject

to a serious check. Generally, authority to change the level of classification of a document is entrusted to the officers who first classified the respective document, which is clearly inappropriate. Separately, the commission for security of information may extend the duration of classification for a period not to exceed the duration of the original period. The grounds of such a decision are broadly determined: "when the national interests require that."

The procedure for deleting classified information also does not guarantee the right to information. The register of classified documents is not public. Neither do declassified documents become public automatically. Consequently documents can be destroyed without citizens being aware that they had been destroyed. Once the information becomes declassified, which happens automatically when the duration of classification expires and is not prolonged, it must still be kept within the authority for one year. During this year a commission within the authority decides whether to destroy the information or keep it, and asks the commission for security of information to approve the decision. Neither the declassification nor the decision to destroy documents is subject to public announcement, and therefore it is very difficult for a person outside the authority to foresee when documents could be destroyed. This also jeopardizes the exercise of the proclaimed right to appeal such decisions in court.

The AIP also protested against the abolition of the law on access to former state security files, which evidently is a step back. The promise that internal regulations would provide citizens with access to such data proved to be a lie. The regulation was not published and is poorly applied. Individuals seeking protection of their rights now address the AIP for help.

Circumstances in which State Secrets Are Called Upon

The AIP's experience in former years has been that state secrets often are not encountered as grounds for the refusal of information.[71] However, the question about state secrets occurred in 1999 during the war in Kosovo, when journalists in the country reportedly were denied information about the number and location of bomb-proof shelters by a reference to the list of classified information.[72]

This problem reappeared in early 2003 after the debate about a possible war with Iraq and the Bulgarian government's decision to support the United States position in the United Nations Security Council. State secrets also were an issue in late 2002, when the Ministry of Defense undertook actions to destroy some military rockets, and environmental pollution concerns were raised publicly. In 2002, the AIP appealed the Cabinet's denial to disclose the rules on handling state secret information in the era of socialism, passed in 1980.[73]

The Courts

There are a few court cases of interest on this topic. The judgment in the most recent case was delivered on Feb. 5, 2003, when the Supreme Administrative Court (SAC) held, inter alia, that former state security services files do not constitute classified information.[74] The Court found no reason to believe the opposite, since Parliament's 1994 decision declassified that information, and it also is not listed in the annex to PCIA.

The SAC referred to the PCIA in May 2002 when it declared the Cabinet's decision to deny access to the minutes of its first meeting unlawful.[75] The Court stated that if an authority that is governed by the Access to Public Information Act (APIA) invokes Article 13, paragraph 2, item 1 of the APIA (the preparatory documents exemption) as a ground for refusal, the information should satisfy the requirements of the PCIA regarding information that may be classified as an official secret. In this respect, the Cabinet should present a list of precisely determined categories of information as required by Article 26 of the PCIA.

In another case, the SAC held that state financial auditors may not refuse access to information (a financial audit) on the grounds that, "during their job, servants doing audits should keep as official secrets all the information, which they know from their work." The Court found that such a provision is related to the time during which the work is undertaken, and does not justify refusing citizens access to information once the audit is finished. Therefore, "official secret" grounds cannot be used.[76]

CONCLUSION

The main challenge for a country like Bulgaria in relation with the conflict for FOI and national security law and practices is to practically promote the principle that FOI takes precedence. Like other Central and East European states, Bulgaria has a serious background of uncontrolled secrecy and only a slight law and practice of FOI.

The interests of politicians and former security officers may motivate both to turn back to practices of secrecy. What contributes to this is some lack of understanding about, and practice of, FOI standards and attempts to replace them with other aims such as security. It is easy to do that in Bulgaria, given the country's history and environment, in which people feel insecure for several reasons, such as adjustment to a market economy, unemployment, and low pensions.

Old ways of thinking are also problematic. The understanding that information is "secret" (that is, exempted from public scrutiny by its nature) prevails, rather than the view that "classification" must occur as a result of human action in which some rules, based on the principle of harm, are applied.

Foreign policies also contribute to the problem. In cases of war, emergency, or instability, people usually feel insecure and instinctively seek protection. They pay too much, however, when the protection they seek is linked with secrecy that results in a lack of accountability.

NOTES

[1] In socialist times, the state formally recognized the right of everyone to seek, receive, and impart information; it ratified the International Covenant on Civil and Political Rights. However, the state undertook no other steps on the domestic level, where the legislation was radically different and the practices of propaganda and censorship were developed.

[2] Its main stimulus was the pollution in Rousse and Chernobil, where the lives and health of many people were affected. See more in Jouleva, Gergana. 2002. "Bulgaria – The Access to Information Programme: Fighting for Transparency during the Democratic Transition." Available at *http://www.freedominfo.org.*

[3] The press in Bulgaria has not been under regulation, and not even 1 percent is owned by the state, while there always has been intense debate about the independence of national broadcasters.

[4] See the AIP annual reports for 2000, 2001, and 2002 at *www.aip-bg.org*.

[5] In 2002, the Cabinet denied the AIP access to the 1980 regulation on state secrets, although it was not supposed to be in force. The Cabinet claimed that the regulation was classified as state secret.

[6] Romania faced a similar situation. See Goldberg, David. 2002. *Promoting Practical Access to Democracy: A Survey of Freedom of Information in Central and Eastern Europe*. London: Article 19; 21-22.

[7] This could be easily identified in the "reasons" (white paper) of the government.

[8] See the conclusions of *The Year of the Rational Ignorance (Results from a Sociological Survey)* by the AIP in 2002.

[9] The AIP received information from different units, including courts and companies, that the PCIA Commission established under the law on protection of classified information required it to implement the rules for keeping state secrets.

[10] Executives in Bulgaria and probably in Romania respect mostly standards and requirements of the EU and NATO.

[11] One reason is that document C-M (2002) 49 (and before that C-M (55) 15, which was the basic requirement when the laws in Bulgaria and Romania were drafted) is not disclosed. See Toby Mendel's Chapter in this volumne, pp. 18-19. I feel that some words could be added here. The twofold role of NATO requirements should be pointed out. Bulgarian and Romanian legislation did not regulate the scope and procedures of classifying documents entirely before they started to tackle the NATO requirements. Also, they did not define a time limit for classified documents initially. The requirements' most obvious positive aspect was that the legislature passed relatively complete and detailed regulation on secrets with some standards in it. The negative side is that governments used the opportunity to broaden the scope of secret information too much. Together, these two factors contributed to this: new legislation was adopted, and the governments are not completely familiar with the NATO guidelines. Some lack of activeness on the part of Parliamentary opposition in Bulgaria also is noteworthy here.

[12] Art. 25 of PCIA states that "State secret is the information determined under the list attached to the act, the unauthorized access to which would endanger or harm the interests of the Republic of Bulgaria related to national security, defense, foreign politics or the protection of the constitutionality established order."

[13] See the 2002 Report of the Romanian Helsinki Committee at *http://www.apador.org/ranuale.htm.*

[14] In Bulgaria, the PCIA repealed the law on access to former state security files. In both Bulgaria and Romania, all of the classified information was put under the same regime, although its scope is far broader than NATO information.

[15] Chapter 2 of the Constitution is devoted to the fundamental human rights.

[16] In its judgementNo. 7 of 1996 on the first constitutional case of 1996.

[17] For details see "Freedom of Information Litigation," ed. AIP, Sofia 2002, p.11-12. Published also on *http://www.aip-bg.org/pdf/court_eng.pdf.*

[18] An authority existing before 1990 and encompassing functions of legislative and executive, and even some of the judiciary.

[19] The law (currently not in force) had a chapter on access to environmental information and provided for both active and passive obligations to disclose information.

[20] See more in "Bulgaria. The Access to Information Programme. Fighting for transparency during the democratic transition,? by Gergana Jouleva, 2002, published on *http://www.freedominfo.org*.

[21] At the end of 1998 and the beginning of 1999, the draft law was announced through the media as a law on state secrets. Later, it was referred to as a law on information.

[22] See also Kashamov, Alexander. 2002. Access to Information Litigation Campaign in Bulgaria." *In The Right to Know, the Right to Live: Access to Information and Socio-Economic Justice*, edited by R. Calland and A. Tilley;

87.

[23] More information of the AIP work these years can be found in Jouleva, 2002, available at *http://www.freedominfo.org*.

[24] During its first year, the AIP established a network of local coordinators in 18 cities/district centers who collected cases (primarily from journalists) and sent them to the AIP. AIP lawyers prepared written legal advice on the cases and returned them to the coordinators, who re-sent them to the affected people and to other interested journalists, NGOs, and officials. Gradually, the network enlarged and now consists of 26 local coordinators, covering all districts in the country except two.

[25] The groups included: the AIP, Bulgarian Helsinki Committee, Article 19, the International Press Institute, the Bulgarian Association of Licensed Broadcasters, the Union of Bulgarian Immigrants in Sweden, and statements from participants in three seminars in the country (local administration, media, and NGOs).

[26] Published in *State Gazette* No. 55 (July 7, 2002).

[27] Some moments of the AIP advocacy campaign were very tentative. An MP from the ruling party at that time, who proposed amendments in the draft law prepared by the AIP, took back the proposal without explanation later on. Another proposal for amendments in the draft, prepared by the AIP and a deputy chair of the Parliamentary Legal Committee from the ruling coalition, was given to the committee members for discussion. Before the next committee hearing, it was revoked silently.

[28] At that time, the AIP thought the definition is rather vague and makes it difficult to determine exactly which information is public. Later, the courts emphasized that problem, but until now, they have not declared any piece of requested information as not within the scope of the APIA.

[29] Pieces of documents could be requested.

[30] There is not a list of authorities that are excluded from the scope of the law. Nevertheless, some authorities have attempted to argue that the APIA does not apply to them (e.g., *Bulgarian Helsinki Committee v. Military Prosecutor of Sliven*).

[31] This term is not defined in the laws. It still is not clear in the doctrine, but it is under interpretation by the courts in some cases involving refusals of the National Health Insurance Fund and the National Electoral Commission.

[32] Under the Constitutional Court interpretation in Decision No. 7 from 1996 on Constitutional Case No. 1 during 1996, "law" means an act of the legislative branch.

[33] This linkage is made in the above-mentioned Constitutional Court Decision. It says that a restriction on the right to information is regarded as an exception from the principle and should pass the following test: (1) to be provided by law, (2) for the protection of the interests precisely enlisted in the Constitution, (3) only to the extent necessary to satisfy that protection (proportionality). The harm test was introduced much later with the Classified Information Act, in May 2002.

[34] This exemption would extend to some period after the final decision is made. The law reads that it cannot be applied after two years from the creation of the document expire (before May 2002 the period was 20 years).

[35] The only time limit was the above-mentioned 20-year period for pre-decisional documents.

[36] The party's parliamentary group probably found that it was unacceptable to have "internal criticism" when the other parties in the Parliament had none.

[37] The Cabinet's legal department representative protested when the work group, which consulted the AIP, introduced its amendments in the Parliamentary Legal Committee. As a result, the committee meeting was postponed and the work group's amendments were repealed silently.

[38] The law on the government's responsibility for harm to citizens (1988) provisions that the administrative courts (two-level system) should declare an administrative act unlawful and only after that one is entitled to compensation, determined by civil courts (three-level system). On average, it takes six to seven years to close a civil case and about two years for an administrative case.

[39] AIP, ed. 2002. *The Year of Rational Ignorance Ignorance (Results from a Sociological Survey)*. Available at www.aip-bg.org.

[40] Ibid., p. 3.

[41] This happened because there was not a specific provision in APIA saying that tacit denials are also subject oto legal review. Possible problem of that kind in Romania was avoided by the provision of Art. 21 Par.1, where tacit denials are referred expressly.

[42] See "Access to Information Litigation in Bulgaria,"18-19. Questioning courts' competence to judge such cases could seem ridiculous from outside, but it stems from the old system of appealing only administrative acts. Omissions are appealed only if the specific law provides so. Court practice on tacit refusals under FOI law was a positive step on the issue as a whole.

[43] The "old fashioned" practice is that courts should consider whether the denial would be in conformity with law if it would be delivered. In such cases, courts previously declared the denials lawful. Two judgments in late 2002 determined that tacit denials under the FOIA seriously infringe the legal requirement for writ-

ten form of the denials as a guarantee to the constitutional right to information. Both are under appeal.

[44] Practically the subject of possible threat was not just nationally, but widely understood. Possible dangers to the USSR as a leader of the socialist camp were practically also under care.

[45] The provision reflects almost explicitly that of Article 83 of the repealed Penal Code (1956). The penalty for imparting state secrets was death or 10 years in prison.

[46] The law required the list to be published, however. The first time it was published was in 1990.

[47] The law was worded otherwise.

[48] In 2001, the Military Prosecution Office started proceedings to investigate a "committed crime" under Article 360 of the Penal Code. A police directorate spokesperson told media that a well-known person was detained and would undergo medical expertise. Luckily, the proceedings were closed soon after that without consequences.

[49] Adopted with a Decree No. 324 from 1994 of the Cabinet, Official Gazette No 5/1995. Repealed by the Regulation on Application of the Law on the Ministry of Interior, adopted with a Decree No 212 from 24/09/1998, Official Gazette No 113/1998.

[50] From the context of the regulation it follows that by "objects" it is meant places, constructions and premises belonging to entities (organs and organizations).

[51] Formally two different provisions stated that the Cabinet should determine the objects (Art.2) and separately the strategic entitites (Art. 4, Par. 1). However, there is no of the existence of a separate list of strategic objects. There is a possibility that the terms "strategic object" and "strategic entity" practically coincided.

[52] They were enclosed on the ground of Art. 6 of the regulation, which empowered NSS to assist and exercise control on non-government organizations to create, organize and ensure functioning of units of security, to protect state secrets and to ensure issuing of clearances for work in strategic and life saving objects.

[53] Published as an appendix to the Cabinet's Decree No. 210 of 1994, in *Official Gazette* No. 84, 1994.

[54] In fact, one of the first steps of the new government was to abolish the legal requirement to publish the list. Decree No. 210 was suspended with a decree on Dec. 28, 1994, published in *Official Gazette* No. 5, 1995.

[55] See "The NEC Case," available at *http://www.aip-bg.org*.

[56] See "Access to Information: Norms and Practices." 1998. Sofia. Available at http://www.aip-bg.org.

[57] See "Freedom of Information Litigation," ed. AIP Sofia, 2002 (cf. note 18 above).

[58] With Decision No 457 of May 2, 1997, of the Council of Ministers.

[59] The problem related to the presence of the Russian Company Gasprom on Bulgarian market.

[60] The preparatory work started in 1999 and the inter-agency work group was appointed on Sept. 20, 2000 (see government reasons [white paper] to the draft).

[61] Cabinet Kostov (1997-2001) and Cabinet Koburgotski (2001-present). The government decided to apply for NATO membership under No. 192 on Feb. 17, 1997. The National Program for Preparation and Association to the Pact was established as a result.

[62] They did this despite the fact that only one MP voted for the publicity of the register before that in Parliament. Probably they liked to have good image before public after AIP strongly criticized the vote on the publicity of the register.

[63] AIP had presented a month ago to UDF MPs its remarks on the law's constitutionality. Its opinion stated that classifying volumes that contain documents that do not need to be classified violates the constitutional right to access information.

[64] Article 25, paragraph 2 of the regulation.

[65] Ibid.

[66] Article 25 of the Protection of Classified Information Act.

[67] See the Executive Order 12958 of 517 April, 1995 on classified national security information, which states that national security is nothing more than the combination of defense and foreign relations (Section 1.1.a).

[68] The recent changes in privatization law removed judicial review on privatization deals related to national security. The broad definition allows every possible interest to be claimed as such of "national security."

[69] In the supplementary provisions, units that have authorization to work with classified information (consequently, to classify) also could be firms.

[70] Evidently, people without training can classify documents, even judges. The AIP was addressed by a woman, who told the group that the court file of her property rights dispute was classified.

[71] See the AIP annual report, "Access to Information Situation in Bulgaria in 2001," available athttp://www.aip-bg.org.

[72] The AIP receives a monthly report of FOI cases from its coordinators in 26 district towns in the country. The reporters are local journalists, an NGO activist, and AIP local coordinators. For more information about the AIP network, see Jouleva, 2002, and AIP annual reports at http://www.aip-bg.org.

[73] The case is pending before the Supreme Administrative Court, Fifth Division.

[74] Decision No. 974 of 2003 on Case No. 11111 of 2002. This was a dispute between the commission under Article 4 of the repealed law on access to former state security services files and the commission under PCIA on the question of the possession of the archive of the documents, possessed by the first commission.

[75] Decision No. 4694 of 2002 on Case No. 7189 of 2001.

[76] The decision is not as good as a whole, since it suggests a ground of a refusal on another ground, but that is out of the scope of the current text.

NATO'S SECURITY OF INFORMATION POLICY AND THE RIGHT TO INFORMATION

Alasdair Roberts[1]
Director, Campbell Public Affairs Institute
The Maxwell School of Syracuse University

In December 2001, the international movement for open government marked a small victory: Romania's new right-to-information statute, the Law Regarding Free Access To Information of Public Interest, came into force. Unfortunately, the victory was soon qualified. In April 2002, Romania adopted a new state secrets law that creates a broad authority to withhold information that has been classified as sensitive by government officials.

Non-governmental organizations complained about the haste with which the state secrets law was adopted, as well as its drafting. The first version of the law was struck down on procedural grounds by Romania's Constitutional Court in April 2001. A second version, although revised in response to criticisms, still proved objectionable. The International Helsinki Federation said that the law "failed to strike a proper balance" between secrecy and the public's right to know. ARTICLE 19, a freedom of expression advocacy group, said that "incredibly broad" restrictions in the law could "substantially undermine" the new right-to-information statute.[2]

Romania is not an unusual case. Ten countries in Central and Eastern Europe have adopted right-to-information laws in the last decade — but eleven have adopted laws to restrict access to information that has been classified as sensitive (Table One). Complaints about undue haste and poor drafting have arisen in several of these countries. The Hungarian

Helsinki Committee complained that Hungary's state secrets law, first adopted in 1995, became problematic after the addition of "extremely vague wording" about classification of information in December 1999. In Slovakia, protests from non-governmental organizations compelled the Cabinet to withdraw a proposed secrecy law in February 2001.[3] A law was eventually adopted in May 2001.

ARTICLE 19 also complained about "absurdly broad" restrictions in the proposed Bulgarian secrecy law. Other critics suggested that the law, eventually adopted in April 2002, might weaken the accountability of the state security service. In May 2002, a cross-party coalition of legislators launched a court challenge, claiming that the law conflicted with Bulgaria's constitutional guarantee of a right to information.[4]

The spread of state secrets laws has also led to strict policies on security clearances. In 1999, Poland's ombudsman questioned the constitutionality of rules in the country's new Classified Information Act that determined which public officials would receive access to sensitive information. Polish judges complained about intrusive investigations to determine whether their lifestyles could make them "susceptible to . . . pressure." Slovakia's the new security agency will review political and religious affiliations, and lifestyles — including extramarital affairs — that are thought to create a danger of blackmail. The Associated Press reported that Romania intends to deny clearances to security staff with "anti-western attitudes."[5]

There is a simple explanation for this wave of legislative activity. In 1999, the North Atlantic Treaty Organization (NATO) said that countries that wanted to join the alliance would need to establish "sufficient safeguards and procedures to ensure the security of the most sensitive information as laid down in NATO security policy." Central and Eastern European countries rushed to get legislation in place before NATO's meeting in Prague in November 2002, where decisions on expansion were expected to be made. The sense of urgency was conveyed in a Romanian news report on the legislative debate in April 2002:

> [On April 3] a certain Colonel Constantin Raicu [of the Romanian Intelligence Service], who is in charge of the protection of state secrets, came down like a storm on the members of the Senate

TABLE ONE
RIGHT-TO-INFORMATION LAWS AND STATE SECRETS LAWS IN CENTRAL AND EASTERN EUROPE[6]

COUNTRY	NATO STATUS†	RIGHT TO INFORMATION LAW	STATE SECRETS LAW
Albania	Candidate	Law on the Right to Information for Official Documents, 1999	Law on Creation and Control of Classified Information, 1999
Bulgaria	Candidate	Access to Public Information Act, 2000	Classified Information Protection Act, 2002
Czech Republic	1999	Law on Free Access to Information, 1999	Protection of Classified Information Act, 1998
Estonia	Candidate	Public Information Act, 2000	State Secrets Act, 1999; amended, 2001
Hungary	1999	Act on the Protection of Personal Data and Disclosure of Data of Public Interest, 1992	Act on State and Official Secrets, 1995; Amended 1999
Latvia	Candidate	Law on Freedom of Information, 1998	Law on State Secrets, 1997
Lithuania	Candidate	Law on Provision of Information to the Public, 2000	Law on State Secrets, 1995
Macedonia	Candidate	None	Not available
Poland	1999	Act on Access to Information, 2001	Classified Information Protection Act, 1999
Romania	Candidate	Law Regarding Free Access to Information of Public Interest, 2001	Law on Protecting Classified Information, 2002
Slovakia	Candidate	Act on Free Access to Information, 2000	Law on Protection of Classified Information, 2001
Slovenia	Candidate	None	Classified Information Act, 2001

Juridical Commission, telling them: "This morning we have received signals from Brussels indicating that if the bill on classified information is not passed before 16 April, they cannot exclude adopting a critical attitude regarding Romania. We agree with any form — the colonel added — but please, pass it as soon as possible, or we will be facing huge problems." The senators . . . grasped the situation very quickly, and they approved the draft bill in the form passed by the Chamber of Deputies.[7]

WHAT IS NATO'S POLICY?

Governments throughout Central and Eastern Europe have said that their legislation is tailored to suit NATO requirements.[8] However, observers have asked whether governments in the region are using the process of NATO expansion as a pretext for adopting unnecessarily broad laws — or whether NATO's requirements are themselves unduly tilted against transparency. These are reasonable questions, but NATO has done little to provide answers. Its security of information (SOI) policy is not publicly accessible. However, available evidence does suggest that the policy —crafted in the early years of the Cold War — is unduly tilted toward secrecy.

For most of NATO's history, its SOI policy was contained in a document known as C-M(55)15(Final), Security within the North Atlantic Treaty Organization. This document had three components. The first and oldest component was a Security Agreement adopted by parties to the North Atlantic Treaty in January 1950. This became Enclosure "A" of C-M(55)15(Final). A second component, first adopted in 1950 but substantially revised over the next five years, outlined detailed security procedures for the protection of NATO classified information. This became Enclosure "C" of C-M(55)15(Final). A third component, adopted for the first time in 1955, had a broader reach. It outlined "basic principles and minimum standards" that were to govern the overall design of national security systems. This affected the handling of all sensitive information, whether provided by NATO or not. This became Enclosure "B" of C-M(55)15(Final) (See Table 2).

The strictness of NATO's SOI policy may be illustrated by its treatment

of the policy itself. Although C-M(55)15(Final) was an unclassified document, NATO refused for decades to make it publicly available. A narrow glimpse of NATO policy may have been provided in 1998, when a revised version of the Security Agreement — which apparently still constitutes Enclosure A of the policy — was made publicly available by NATO member states.[9] Versions of C-M(55)15(Final) adopted before 1964 have also been made available in the NATO Archives.

Nevertheless, the complete and current version of C-M(55)15(Final) remained inaccessible. In February 2002, NATO's Security Office refused access to the document, explaining that "NATO unclassified information . . . can only be used *for official purposes*. Only individuals, bodies or organizations that require it for official NATO purposes

TABLE TWO
COMPONENTS OF NATO'S
SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANIZATION

	C-M(55)15(Final)†	**C-M(2002)49 (June 2002)**
Enclosure "A"	Security Agreement	Security Agreement
Enclosure "B"	Basic Principles and Minimum Standards of Security	Basic Principles
Enclosure "C"	Security Procedures for Protection of NATO classified information	Personal Security
Enclosure "D"	Industrial Security	Physical Security
Enclosure "E"	Protection Measures against Terrorist Threats††	Security of Information
Enclosure "F"		INFOSEC†††

† Titles for Enclosures "A" to "D" are based on the version of C-M(55)15(Final) issued in July 1964.
†† This title is based on information in Canadian government documents released in response to an Access to Information Act request. Apparently revised in March 2002.
††† INFOSEC relates to the identification and application of security measures to protect information processed, stored or transmitted in communication, information and other electronic systems.

may have access to it."[10] NATO also instructed member countries to withhold their copies of C-M(55)15(Final). As a result, requests for the policy made under several national right-to-information laws have been refused.

NATO began an overhaul of C-M(55)15(Final) in the late 1990s. The review, guided by an Ad-Hoc Working Group for the Fundamental Review for NATO Security Policy, was completed in early 2002. A revised security policy, now known as C-M(2002)49, was adopted by NATO on June 17, 2002. The Working Group completed its work in secrecy, and the new policy remains inaccessible to the public[11], although its outlines can be reconstructed from other sources (Table 2).

NATO's reticence means that an assessment of its SOI policy must be largely speculative. Nevertheless it is possible, from archival and other sources, to describe the policy in broad terms. It has five basic features, each designed to ensure a high level of security for information.

Breadth. The first of these elements might be called the principle of breadth, although this term is not used in NATO documents. It implies that the policies that a member state adopts regarding security of information should govern all kinds of sensitive information, in all parts of government. It eschews narrower approaches, perhaps limited to information received through NATO, or information held within military or intelligence institutions. The principle is expressed in the 1964 edition of C-M(55)15(Final), which articulates standards for information security that apply to all sectors of government, on the grounds that member states must be assured that each country gives "a common standard of protection . . . to the secrets in which all have a common interest."[12]

Depth. The next principle underpinning NATO policy is that of depth of coverage, although again the principle is not expressed in this way in NATO documents. The policy errs on the side of caution when determining what information should be covered by SOI rules. This is evident in the NATO classification policy, whose lowest category — RESTRICTED — applies to information whose relevance to security is negligible. The next highest category — CONFIDENTIAL — relates to information "the unauthorized disclosure of which would be prejudicial to the interests of NATO"; RESTRICTED information does not need to meet even this test.[13] (Several CEEC countries have adopted

equally broad classifications for the whole of government. Under Czech law, for example, information is classified as RESTRICTED if disclosure would be unfavorable to the Republic14; in Slovenia, information is RESTRICTED if disclosure could harm the activity or performance of tasks of an agency.[15])

Centralization. A third principle of NATO policy is that of centralization. This has a national and intergovernmental aspect. At the national level, centralization of responsibility and strong coordination are regarded as "the foundations of sound national security". Member states are expected to establish a "national security organization" (NSO) that is responsible for the security of NATO information and screening of personnel; for "the collection and recording of intelligence regarding espionage, sabotage and subversion"; and for advice to government on threats to security and appropriate responses. The NSO must also have the authority needed to conduct inspections of security arrangements for the protection of NATO information within other departments and agencies, and to investigate and respond to breaches of security.[16]

This structure is roughly replicated at the intergovernmental level. In 1955 the North Atlantic Council gave its Security Bureau the responsibility for "overall coordination" of security in NATO. The Security Office, as it is now known, advises national authorities on the application of principles and standards, and carries out surveillance of national systems to ensure that NATO information is adequately protected. National authorities have an obligation to report possible breaches of security to the NATO office.[17]

Controlled distribution. The NATO security policy also invokes two rules that are intended to strictly control the distribution of information. The first of these is "the NEED TO KNOW principle": that individuals should have access to classified information only when they need the information for their work, not "merely because a person occupies a particular position, however senior." This is regarded as a "fundamental principle" of security. Judgments about whether an individual has a "need to know" are made by the originator of the document, or by one of the addressees identified by the originator.[18]

The second rule that restricts the distribution of information may be called the principle of originator control. The principle acknowledges

the right of member states, and NATO itself, to set firm limits on the distribution of information that is circulated among member states. Such information may not have its classification reduced, or be declassified, without the consent of the government from which the information originated.[19] As a consequence, the principle of originator control trumps the "need-to-know" principle, since originators may impose a high level of classification that restricts the number of individuals to whom the document might be referred by an addressee.

The principle is even stricter with regard to distribution of documents outside the community of NATO governments. In this case, distribution is absolutely prohibited without consent, even if the information is unclassified. In these circumstances, the information is regarded as "the property of the originator," which retains absolute control over its distribution.[20]

Personnel controls. The fifth and final element of the NATO security policy comprises strict rules regarding the selection of individuals who are entitled to view classified information. The precise requirements for personnel screening are not easy to discern. Some of the exact criteria adopted during the Cold War are probably no longer applicable; and some of the criteria used in NATO's early years continue to be withheld.[21]

The policy relies on a system of "positive vetting," in which individuals who handle sensitive information are subjected to active background investigation before receiving clearance. NATO's early policy made clear that decisions could be based on assessments of character and lifestyle, and that the evidentiary burden for denying clearances was low. Individuals were expected to demonstrate "unquestioned loyalty [and] such character, habits, associates and discretion as to cast no doubt upon their trustworthiness."[22]

Other controls are imposed to control personnel after a clearance has been provided. C-M(55)15(Final) stipulated that supervisors should have a duty "of recording and reporting any incidents, associations or habits likely to have a bearing on security." Evidence that created a "reasonable doubt" about loyalty or trustworthiness required the removal of a security clearance. There is also an expectation that "disciplinary action" will be taken against individuals who are responsible

for the unauthorized disclosure of information, and that there will be clear criminal penalties for unauthorized disclosure.[23]

CONSTRAINTS ON NATIONAL POLICIES

Of course, it is not surprising that NATO — as an organization whose mission is the promotion of collective security — should seek to establish strict rules on the handling of sensitive information within the governments of its member states. But there are also special historical reasons that may explain the strictness of NATO's SOI policy.

The policy was codified between 1953 and 1955, in the early and hardest years of the Cold War. Military planners played the leading role in defining the policy, sometimes overriding civilian policymakers in other governments who considered that military SOI standards were excessive.[24]

The policy was also shaped by domestic politics within the United States. The anti-communist crusade reached its zenith in 1954, with Senator Joseph McCarthy's hearings into alleged Communist subversion in the U.S. Army, and the hearings that led to the revocation of the security clearance of J. Robert Oppenheimer, former director of the Manhattan Project, because of "fundamental defects in his 'character'." The Eisenhower Administration was determined to avoid the criticism over internal security that had undermined President Truman's 1952 election campaign, and had boasted in January 1954 that new loyalty rules had already resulted in the dismissal of over two thousand federal employees. This preoccupation with internal security was reflected in the American government's approach to the adoption of NATO policy in 1954-55.[25]

The difficulties created by the export of demanding SOI rules were evident to other NATO governments. For several years after the establishment of NATO in 1948, the British government resisted American pressure to adopt positive vetting procedures like those contained in the domestic "loyalty program" introduced by the Truman administration in 1947. Many British policymakers found American methods severe and distasteful, and doubted their effectiveness. They preferred a less comprehensive system — "negative vetting" — combined with stricter

criminal sanctions for unauthorized disclosure of information. The disagreement meant that rules on positive vetting were not included in early versions of NATO's SOI policy.

However, the British government capitulated in 1952. Its position had been undermined by the Burgess and McLean defections, and the American government had made clear that positive vetting was essential if the British government expected to receive information on the development and deployment of nuclear weapons. The British government affirmed its commitment to a screening process that searched for evidence of character defects or "loose living" that might make individuals susceptible to pressure. It conceded that the new policy was "alien to our traditional practices," but argued that individual rights had to be subordinated to the need for state security. [26]

NATO's archival records show that other concerns were expressed as C-M(55)15(Final) was prepared for adoption. The Canadian government feared that the new policy might give the NATO Security Bureau an inappropriate role in shaping national security policies. The Danish government expressed its concern about the breadth of the new policy, suggesting it overreached by attempting to set rules on the handling of non-NATO information. The Italian government suggested that the breadth of policy might create "difficulties of a constitutional nature." Nevertheless, the scope of the policy was not changed. [27]

Similarly, complaints about the depth of the new policy were aired but defeated. In January 1955, the Norwegian government proposed that the classification system should be simplified by eliminating the lowest security grading for information, RESTRICTED. It argued that the definition of the RESTRICTED category and rules governing the use of RESTRICTED information "were so vague that they might lead to confusion instead of contributing to overall NATO security." A majority of other nations disagreed, and "for the sake of unity" Norway withdrew its proposal.[28] In October 1957, the Danish government once again proposed a simplification of the grading system, which it said encouraged over-classification.[29] Again, a majority of other countries vetoed the proposal. The record of the July 1958 meeting of the Security Committee at which the Danish proposal was rejected is still withheld by NATO.[30]

Because of NATO's unwillingness to release internal documents produced after 1964, it is impossible to know how the debate over SOI policy continued in later years. But it seems certain that there must have been further contention over the policy. One reason would be the diffusion of right-to-information laws among NATO member states. Before 1966, no NATO state had a right-to-information law; by 2001, sixteen of the nineteen states had adopted such statutes. [31] These laws are typically founded on principles that are completely at odds with the restrictive rules on dissemination of information contained within NATO policy.

The tension between international obligations and domestic expectations is sometimes evident in debates over national right-to-information laws. For example, the British government was careful to accommodate the principle of originator control, a basic feature of NATO SOI policy, within its proposed Freedom of Information Act of 1999.[32] The non-governmental Campaign for Freedom of Information criticized this as one of several "indiscriminate" exemptions that would allow the withholding of "harmless information", but the government opposed attempts to remove the provision. [33] Similar complaints were made against the comparable provision in the proposed Scottish freedom of information bill; however, the Scottish Executive was also explicitly constrained — by the agreement governing the delegation of power to Scotland from the United Kingdom — to respect the terms of C-M(55)15(Final), and the provision remained intact. [34]

The Canadian government has also resisted efforts to weaken the originator control rule contained in its 1982 Access to Information Act. In 2002, it argued that any weakening of this provision would "set Canada apart from its key allies."[35] In fact, the government recently amended the 1982 law so that it would be allowed to eliminate a right of appeal against its decisions to withhold information received from allies.[36] Internal memoranda suggest that the highly contentious amendment was the product of bureaucratic frustration with requests for information that were governed by rules such as those in NATO's SOI policy.[37]

Similarly, NATO policy has had a controversial impact on the access to information policy of the European Union. The EU adopted its first code on access to documents in December 1993. However, the code was substantially revised in August 2000. A large number of classified

documents were wholly excluded from the code on access of documents, and the Council's discretion to withhold other documents relating to security matters was broadened. At the same time, the Council hardened its policy on control of classified information.[38]
Many observers were shocked by these changes, protesting that the Council had executed a "summertime coup" against transparency. However, the Council's decisions proved to be prerequisites for a cooperation agreement with NATO signed in July 2000, in which the Council agreed to comply with the requirements of C-M(55)15(Final).[39]

The spirit of the August 2000 amendments was carried forward into a new regulation governing access to information held by EU institutions adopted in May 2001. Under the new regulation, national governments and institutions such as NATO retain the right to veto disclosure of classified information relating to public security or defense which they have provided to the EU. The classification policy of the authoring institution, rather than that of the EU, will determine whether documents are subject to the rule of originator control.[40] These arrangements were unpopular among advocates of transparency but clearly consistent with NATO requirements.

The impact of EU-NATO cooperation expanded in March 2001, when new security regulations governing EU classified information were approved by the Council. The regulations replicate NATO SOI rules. The span of these regulations is not limited to EU institutions: member states also have an obligation to adopt "appropriate national measures" to ensure that the Council's rules on the handling of classified information are respected within their governments.[41] This imposes another constraint on the transparency policies of the fifteen EU member states — and on the policies of those Central and Eastern European states that hope to join the European Union at its December 2002 summit.[42]

WEB OF SECRETS

It can now be seen that the controversies over new state secrets laws in Central and Eastern Europe are not unusual. Rather, they may be part of a decades-long process through which the national policies of NATO member states, and allied institutions such as the European Union, have been reshaped to conform to NATO's SOI requirements.

This process of policy rationalization is deeply problematic. In some respects, NATO's SOI policy does not appear to strike a reasonable balance between security concerns and other critical considerations, such as the need to ensure accountability through a right of access to government documents.[43] Rather, NATO policy appears to perpetuate an approach forged in the hardest years of the Cold War, when citizens had more modest expectations regarding governmental transparency. Of course, this may be a mistaken view of NATO's current policy. It is difficult to be sure when the policy itself is inaccessible.

Two conclusions should be drawn from this discussion. The first is the need to be chary of claims about advances in government transparency over the last decade. It is true that the number of right-to-information laws has increased substantially over the last decade.[44] Slow but significant reforms at major international institutions[45] might seem to suggest that intergovernmental organizations are also recognizing an obligation to conform to standards of transparency comparable to those imposed on national governments. These are important advances; however, we must weigh against them the impact of processes of defense and intelligence integration. The drive to promote collective security has produced a thickening web of intergovernmental commitments on the handling of sensitive information, that entrench norms that are hostile to the principle of governmental transparency.

The experience of CEE countries with NATO policy also reminds us of a larger point: the need to ensure an appropriate balance between security concerns and democratic accountability. No one can dispute that the preservation of secrets is sometimes essential to national security. But at the same time, such secrecy compromises the capacity of citizens to monitor and control the actions of their governments. The best response to this dilemma, Dennis Thompson has argued, is to ensure that there is proper public discussion of the rules that determine when secrets shall be kept. "Secrecy is justifiable," Thompson says, "only if it is actually justified in a process that itself is not secret. First-order secrecy (in a process or about a policy) requires second-order publicity (about the decision to make the process or policy secret)."[46]

NATO's SOI policy flouts this basic principle of accountability. The rights of citizens in NATO member states are clearly affected by NATO rules. NATO requirements constrain their right to government docu-

ments, and their ability to obtain security clearances and government employment. Nevertheless the policy — even though unclassified — remains inaccessible to citizens. Nor are citizens able to participate in, or observe the processes by which the content of this policy is determined. Indeed, they are not even informed when the policy is subject to revision, as it was during the last few years. This is an indefensible level of secretiveness. The habit of secrecy which has driven NATO's conduct should be broken, and the key elements of its SOI policy should be laid open for public review.

ENDNOTES

[1] This article first appeared in *East European Constitutional Review*, 11.3/4 (2003). It is reproduced with permission. A more extensive version of the argument can be found in Alasdair Roberts, "Entangling Alliances: NATO's Security Policy and the Entrenchment of State Secrecy." *Cornell International Law Journal* 36, no. 2 (2003).

[2] International Helsinki Federation, *Human Rights in the OSCE Region: Report 2002* (Vienna: International Helsinki Federation, 2002), 257; ARTICLE 19, *Memorandum on the Romanian Law for the Protection of Classified Information* (London: ARTICLE 19, 2002), 2, 8.

[3] International Helsinki Federation, *Human Rights in the OSCE Region: Report 2000* (Vienna: International Helsinki Foundation, 2000), 185; Alex Grigorescu, "European Institutions and Unsuccessful Norm Transmission: The Case of Transparency," *International Politics* 39, no. 4 (2002).

[4] ARTICLE 19, *Memorandum on the Bulgarian Law on the Protection of Classified Information* (London: ARTICLE 19, 2001); Ulrich Buechsenschuetz, "Bulgaria's New Law on Classified Information," *RFE/RL Newsline*, April 30, 2002; Radio Free Europe, "Opposition Appeals to Constitutional Court over Law on Classified Information," *RFE/RL Newsline*, May 30, 2002.

[5] International Helsinki Federation, *Human Rights in the OSCE Region: Report 2000*, 286; International Helsinki Federation, *Human Rights in the OSCE Region: Report 2001* (Vienna: International Helsinki Federation, 2001), 240; Radio Free Europe, "Polish Judges under Secret Service Surveillance," *RFE/RL Newsline*, August 11, 2000 2000; Peter Sobcak, "New Security Office to Guard NATO Secrets," *Slovak Army Review*, Spring 2002; Associated Press, "NATO Officials Want Romania to Exclude Some Former Communists from Intelligence Positions," *Associated Press*, March 20, 2002.

[6] Status at November 15, 2002. The main source for this table is David Banisar, *Freedom of Information and Access to Government Records around the World* (London: Privacy International, 2002).

[7] NATO, *Press Release: Membership Action Plan* (Brussels: NATO, 1999); Bucharest Ziua, "NATO Used as Scarecrow to Pass Law on Secrets," *Bucharest Ziua*, April 8, 2002.

[8] It is reported that Bulgaria's foreign minister defended the country's proposed state secrets law by saying that NATO experts had described it as one of the best statutes of its type among all NATO applicant countries: Radio Free Europe, "Bulgarian Parliament Starts Vote on Classified Information Protection Law," *RFE/RL Newsline*, April 18, 2002.

[9] The Canadian Government published the revised agreement, the *Agreement between the Parties to the North Atlantic Treaty for the Security of Information*, as Canada Treaty Series document 1998/56.

[10] Office of Security, Letter from Mr. Wayne Rychak, Director, to Mr. Jacob Visscher, General Secretariat of the Council of the European Union (Brussels: NATO Office of Security, 2002). Emphasis in original.

[11] The existence of the Working Group was acknowledged in Canadian government documents released to the author in response to a request under Canada's Access to Information Act in September 2002. The first public acknowledgement of the existence of the new policy by NATO was made in September 2002: see http://www.shape.nato.int/BUDFIN/UPDATE%20IFIB.htm (Downloaded October 30, 2002).

[12] NATO, *Security within the North Atlantic Treaty Organization* (Brussels: NATO Archives, 1964), Enc. B, Para. 1.

[13] NATO, *Security within the North Atlantic Treaty Organization*, Enc. C, Sec. II.

[14] Protection of Classified Information Act, 1998, section 5(5).

[15] Classified Information Act, article 13.

[16] NATO, *Security within the North Atlantic Treaty Organization*, Encl. B Para. 3, Encl. C Sec. I Para. 15; and Sec. IX, Paras. 3-5.

[17] NATO, *Security within the North Atlantic Treaty Organization*, Encl. C Sec. I Para. 3 and Sec. IX, Para. 4. NATO documents refer to periodic inspections of national systems. "Surveillance" is the term used to describe comparable oversight arrangements in other multilateral agreements, such as the Article IV consultations undertaken by the International Monetary Fund, and the trade policy reviews undertaken by the World Trade Organization.

[18] Security Committee, *A Short Guide to the Handling of Classified Information* (Brussels: NATO Archives, 1958), 4; Emphasis in original. NATO, *Security within the North Atlantic Treaty Organization*, Enc. B, Introduction, Para. 5(d), Sec. VI, Paras. 6-7, and Sec. VIII, Paras. 4-5.

[19] NATO, *Security within the North Atlantic Treaty Organization*, Enc. C, Sec. V; NATO, *Agreement between the Parties to the North Atlantic Treaty for the Security of Information*, Article 1.

[20] NATO, *Security within the North Atlantic Treaty Organization*, Enc. C, Introduction.

[21] These appear to be contained in a Confidential Supplement that was added to C-M(55)15(Final) in January, 1961. Archival copies of the Supplement are not

accessible, but a sense of its content can be obtained from the Index to C-M(55)15(Final).

[22] The 1964 policy observes that "fullest practicable use should be made of the technique of background investigation" NATO, *Security within the North Atlantic Treaty Organization*, Encl. B, Para. 9.

[23] NATO, *Security within the North Atlantic Treaty Organization*, Enc. B, Paras. 11-15 and Encl. C, Sec. IX, Para. 10. On criminal penalties, see Alasdair Roberts, "Entangling Alliances: NATO's Security Policy and the Entrenchment of State Secrecy."

[24] For further discussion, see Roberts, "Entangling Alliances: NATO's Security Policy and the Entrenchment of State Secrecy."

[25] Edward Shils, *The Torment of Secrecy* (Chicago: Ivan R. Dee, 1996), 214; Athan Theoharis, *Chasing Spies* (Chicago: Ivan R. Dee, 2002); Richard Polenberg, *In the Matter of J. Robert Oppenheimer: The Security Clearance Hearing* (Ithaca: Cornell University Press, 2002), 380; Richard Rovere, *Senator Joe McCarthy* (New York: Harcourt Brace Jovanovich, 1959), 17-18.

[26] United Kingdom, "White Paper on Security Precautions in the British Civil Service," *Public Administration* 35 (1957), 297-304. On the evolution of British policy, and American pressure to adopt positive vetting, see Margaret Gowing, *Independence and Deterrence: Britain and Atomic Energy*, 1945-1952, 2 vols. (New York: St. Martin's Press, 1974), Vol. 1; Richard Aldrich, *The Hidden Hand: Britain, America and Cold War Secret Intelligence* (New York: The Overlook Press, 2002), David Vincent, *The Culture of Secrecy in Britain*, 1832-1998 (New York: Oxford University Press, 1998), 204.

[27] Canada, *Memorandum to Council from Canadian Government on Proposed Security Regulations*, February 24, 1955. C-M(55)25 (Brussels: NATO Archives, 1955); NATO, *Note by the Secretary General and Vice-Chairman of the Council on Security Procedures for the Protection of NATO Classified Information*, March 8, 1955, C-M(55)15(Final) (Brussels: NATO Archives, 1955), Security Committee, *Summary Record of NATO Security Committee* Meeting, January 24-28, 1955, February 8, 1955. AC/35-R/11 (Brussels: NATO Archives, 1955), 1.

[28] Security Committee, *Summary Record of NATO Security Committee Meeting, January 24-28, 1955*, February 8, 1955. AC/35-R/11; North Atlantic Council, *Summary Record of Meeting of the Council on March 2, 1955*, C-R(55)8 (Brussels: NATO Archives, 1955).

[29] NATO, *Summary Record of Meeting of the NATO Security Committee*, October 17-18, 1957. AC/35-R/22 (Brussels: NATO Archives, 1957); Denmark, *Memorandum to the NATO Security Committee on Controlling and Reducing*

the Volume of Classified Information and Documents, January 11, 1958, AC/35-D/226 (Brussels: NATO Archives, 1958).

[30] The withheld document is NATO AC/35-R/23, the summary record of the meeting of the NATO Security Committee held on July 16-17, 1958. A working group on the control of the volume of classified documents in NATO agencies had earlier reported that a majority of its members opposed the Danish proposal. NATO, *Note by Chairman of the Working Group on the Control of Classified Documents in NATO Agencies*, January 13, 1958, AC/35-WP/13 (Brussels: NATO Archives, 1958).

[31] The first law was adopted by the United States in 1966. Today, the three exceptions were Germany, Luxembourg and Turkey.

[32] The originator rule is preserved in section 27(3) of the Freedom of Information Act, 2000.

[33] Campaign for Freedom of Information, *Briefing for MPs for the Report Stage Debate on the Freedom of Information Bill* (London: Campaign for Freedom of Information, 2000); House of Lords, *Hansard*, November 14, 2000. Vol. 619, Part 166.

[34] Scottish Executive, *Concordat between the Scottish Ministers and the Secretary of State for Defence* (Edinburgh: Scottish Executive, 2000).

[35] Access to Information Review Task Force, *Access to Information: Making It Work for Canadians* (Ottawa: Treasury Board Secretariat, 2002), 51.

[36] The new restrictions were contained in the Anti-Terrorism Act adopted in December 2001. The minister responsible justified the restrictions by telling Parliament that "our allies . . . will not provide us with information . . . unless we can provide them with a guarantee of confidentiality." Hon. Anne McLellan, Minister of Justice, *Hansard*, October 17, 2001.

[37] Alasdair Roberts, "Canadian Officials Use September 11 as Excuse to Restrict Access to Information," *Winnipeg Free Press*, October 8, 2002.

[38] Council of the European Union, *Council Decision* 2000/527/EC, *Amending Decision* 93/731/*Ec on Public Access to Council Documents* (Brussels: Council of the European Union, 2000); Council of the European Union, *Decision of the Secretary-General of the Council/High Representative for Common Foreign and Security Policy on Measures for the Protection of Classified Information Applicable to the General Secretariat of the Council* (Brussels: Council of the European Union, 2000).

[39] Tony Bunyan, "Secrecy and Openness in the European Union," *freedominfo.org*, October 1, 2002, Chapter 6. The EU's letter of agreement with NATO was released in February 2002 in response to a right-to-information request by Swedish researcher Ulf Öberg — with the specific reference to NATO's security policy carefully excised. (The Secretary General of the EU, Javier Solana, is also a former Secretary General of NATO.)

[40] European Union, *Regulation* (EC) 1049/2001 *Regarding Public Access to European Parliament, Council and Commission Documents* (Brussels: European Union, 2001), Art. 9.

[41] Council of the European Union, Council Decision 2001/264/EC *Adopting Council's Security Regulations* (Brussels: Council of the European Union, 2001), Preamble and Article 2. The European Parliament has challenged the security regulations before the European Court of Justice. The European Commission also adopted the same security regulations on November 29, 2001: Decision 2001/844/EC, ECSC, *Euratom*.

[42] These are Bulgaria, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia and Slovenia.

[43] ARTICLE 19, the Global Campaign for Free Expression, convened a group of experts in 1995 to develop principles on the appropriate balance between national security and transparency. NATO's policy seems to violate several of the practices that are condemned by the so-called "Johannesburg Principles": the categorical denial of public access to information, regardless of importance (Principle 12); punishment for disclosure of information, without regard to harm or benefit from disclosure (Principle 15); and denial of employment because of opinion or beliefs; or denial of due process in removal (Principles 5 and 20). See Sandra Coliver et al., eds., *Secrecy and Liberty: National Security, Freedom of Expression and Access to Information* (The Hague: Martinus Nijhoff Publishers, 1999), 1-10.

[44] Eighteen countries had national right-to-information laws in 1992; 49 countries had such laws in 2002 Banisar, *Freedom of Information and Access to Government Records around the World*.

[45] Such as the World Bank, the International Monetary Fund, and the World Trade Organization. See Alasdair Roberts, "A Partial Revolution: The Diplomatic Ethos and Transparency in Intergovernmental Organizations." *Public Administration Review* (Forthcoming).

[46] Dennis Thompson, "Democratic Secrecy," *Political Science Quarterly* 114, no. 2 (1999): 185.

ACCESS TO INFORMATION AND NATIONAL SECURITY IN CHILE

Felipe González,[1] **Professor of Constitutional Law**
Diego Portales University

BACKGROUND AND CONTEXT

As in most Latin American countries, in Chile the issue of national security was the main focus of the public agenda for several decades. The issue expanded mainly as a result of the dissemination of the so-called "national security doctrine" throughout the region. First conceived by the U.S. Armed Forces, this concept was disseminated on a large scale by the School of the Americas, at which several generations of top-ranked military officers from Latin American countries were indoctrinated. The national security doctrine was envisioned as a central tool in the context of the Cold War, when the Cuban Revolution was considered a major threat to the United States' influence in the region, and it focused the discussion, regulations, and actions in such context. Therefore, according to this doctrine, even threats to national security that came from primarily internal sources (e.g., guerrilla groups or revolutionary parties) were in fact part of a broader, international scenario. Human rights were not seen as part of the national security concept, but instead as a propaganda tool for those who pursued the revolution.

The national security doctrine found a fertile ground in Latin America because, in addition to the Cold War context, the region had some features that connected well with old authoritarian trends, which came from the time when the countries there were Spanish colonies. Most countries had, in fact, enacted harsh regulations on state security well

before the development of the national security doctrine, which severely restricted human rights, including freedom of expression. This was reflected both in the legislation for "normal" situations and in the regulations for States of Exception. Thus, in a way, the national security doctrine strengthened old Latin American features and took them to extremes.

Access to information barely existed as an explicitly recognized right in the constitutions of Latin American countries until a few years ago. It was first necessary for the states of Latin America to ratify treaties such as the International Covenant on Civil and Political Rights and the American Convention on Human Rights, which do recognize that right, before domestic legislation began regulating it.

Chile was no exception. Although Chile has ratified both of the above-mentioned treaties, there is still no explicit mention of the right to information in its Constitution. This is consistent with the traditional features of the country's political system, which historically has embodied a lack of significant transparency and accountability of the state's authorities and by hierarchical conceptions and institutions, whereby those who govern the state enjoy a higher status than the rest of the population.

Over the last few years, during the ongoing transition to a fully democratic system, some developments have taken place in Chile concerning the right of access to information. For instance, despite the lack of express recognition in the Constitution, this right has been pointed out as implicit in that legal text in a series of judicial decisions, the most relevant of which was made by the Constitutional Tribunal in 1995. According to that decision, "This right is implicit in the freedom of opinion and of information, because these freedoms would be worthless if they lacked actual beneficiaries."[2] Additionally, a 1999 law established a procedure for obtaining access to public information. While this legislation has insufficiencies and flaws, it is still an improvement from the prior situation. Nevertheless, the road through the transition has been plagued by many obstacles and steps backward.

It must be noted that although the Constitution in its original text (enacted by the dictatorship in 1980) did not mention international human rights standards, according to an amendment incorporated into the Constitution on the eve of the transition to democracy (after Pinochet

lost a Plebiscite to continue in power), the state has a duty to respect and promote those human rights enshrined in international treaties to which Chile is a party (the International Covenant on Civil and Political Rights and the American Convention on Human Rights are the two most important for this paper). This is provided by Article 5.2 of the Constitution. Consequently, the Constitution has recognized the right of access to information since that amendment was adopted. However, the local courts have developed this idea with regard to just a few rights, and access to information has not been among them. In fact, generally speaking, jurisprudence based on Article 5.2 of the Constitution has been scarce.

CRIMINAL LEGISLATION ON NATIONAL SECURITY AND ITS IMPACT ON ACCESS TO INFORMATION

Chile has a long history of *desacato* laws, that is, crimes of contempt of authority, which have the alleged objective of protecting state security and public order. In fact, provisions of this kind can be found in legal texts from the time when Chile was a Spanish colony. After the country became independent, provisions of this sort were introduced into the penal code and later into the Code of Military Justice. Additionally, during the Twentieth century, a series of special legislations were enacted in this regard. In fact, these special laws have been most usually applied than the codes in this matter. They started with several laws in the 1930s and were followed by the so-called Law for the Defense of Democracy in 1948, which was adopted at one of the peaks of the Cold War. It outruled the Communist and Nazi parties and established harsh penalties for what would otherwise be considered the exercise of rights, such as freedom of expression, freedom of association, labor rights, and others.[3]

The Law for the Defense of Democracy was abrogated by the State Security Law in 1958, which is still in effect. This legislation contained less harsh measures than its predecessor, but it maintained many features of an authoritarian conception of state security and was regularly applied during the three governments prior to the 1973 coup. After the coup, the State Security Law was substantially reformed: many behaviors that were legitimate according to international standards were deemed alleged threats to state security, and very harsh penalties were introduced. This law became one of the dictatorship's most-used tools to repress its opponents.

At the beginning of the transition to democracy during the early 1990s, the government substantially modified this legislation again, this time to make it more compatible with the new political trends. The text that emerged was quite similar to that which existed before the coup.

Since its adoption in 1958, the declared aim of the State Security Law has been to protect the democratic system. However, from the very beginning this legislation lacked enough consideration for human rights, and in applying it the tribunals have expanded the limitations for rights that this law provides. Given the traditional weakness of the Chilean Courts to confront issues with a political impact, the fact that special legislation on national security remains without being incorporated into the criminal code produce a prejudice for human rights protection. Indeed, the courts usually do not consider the general principles of the criminal code when they apply to national security regulations. Many provisions of the State Security Law are vague and overbroad. For instance, Article 4, which regulates crimes against internal state security, punishes a person who attempts to act or in fact acts against the established government *in any way*.

In addition, this law is not clear enough about how it protects the democratic system, although this reportedly was its original purpose. Many of its provisions refer to protecting the "Established Government" (*Gobierno Constituido*). In Spanish, this is an ambiguous expression that means both the political organization of the state and the executive branch. Many provisions of the law, including several concerning freedom of expression, use the words "Established Government," and the courts often have considered only the executive branch.

When applying the provisions of the State Security Law in a specific case, the courts consistently have declared that it is beyond their powers to determine whether national security or public order actually was affected. Consequently, freedom of expression and other rights have been limited further. For regulation of offenses against public order, Article 6 provides: "In the following cases an offense against public order is committed," and enumerates eight situations. This has led to a kind of assumption of criminal responsibility, despite the fact that public order may not have been affected in the specific case before a court.

The courts have stated that:

> Article 6 of the Law [12,927] establishes that those who engage in any of the conducts that the law describes 'commit a crime against the public order.' In this way, it is the law itself that assumes that this crime causes a disturbance of the public order in some way. Therefore, it is not proper for the judge to rule contrary to the explicit wording of the law, which is clear, reaching a different conclusion by way of interpretation.[4]

In addition, the Chilean Courts have failed to implement the Bill of Rights provided in the Constitution in connection with cases involving national security issues. The list of fundamental rights contained in the Constitution would provide guidance for an appropriate reading of the law; however, the courts have tried to implement national security and public order regulations regardless of the constitutional context, rendering the constitutional norms meaningless in this respect.

During the transition to democracy the State Security Law (and, more precisely, its Article 6.b) has been applied in about 30 cases in connection with freedom of expression issues.[5] This has had severe consequences for the quality of the public debate in Chile, producing a "chilling effect." Several factors have contributed to this situation, among them: the fact that the military kept a significant amount of power after the dictatorship and has brought a number of cases under this legislation to the tribunals; the strong concentration of media ownership and the lack of investigative journalism; and, in a more general sense, the fact that old authoritarian features still pervade the Chilean culture, politics, and judges to some extent.

In this context, most of the cases pursued under the State Security Law during the 1990s and in the current decade have been high-profile ones. Pinochet himself started several of them before his detention in London.[vi] Despite the fact that Pinochet was released in the end (first in England and later in Chile), he has become a rather marginal figure in Chilean politics. He has not initiated further actions against his critics, based on neither the State Security Law nor on any other legislation. Many cases brought under the State Security Law during the transition have targeted independent journalists who were conducting investigations on issues of public interest. Others have involved politicians and public figures.

Although, since the beginning of the transition, there was some criticism about applying the State Security Law to freedom of expression cases, the criticisms were not widespread, and for almost a decade most politicians took no action to change the law's application. Indeed, the political class still considered this legislation legitimate by the mid-'90s, as demonstrated in the case against Francisco Javier Cuadra, when both the Chamber of Deputies and the Senate brought judicial actions based on the State Security Law.[7]

A crisis erupted in 1999 when Supreme Court Justice Servando Jordán presented a complaint based on the State Security Law against Alejandra Matus, a journalist who recently had written a book entitled *El Libro Negro de la Justicia Chilena* (*The Black Book of the Chilean Judiciary*). The book criticizes the role the judicial system has played since the 1960s, especially its passivity when massive executions and forced disappearances were taking place during the dictatorship. Justice Jordán, who recently had been under investigation for charges of corruption and having links with drug dealers, argued that the book affected his honor and obtained a preventive order banning its publication. Matus, who was married to an American citizen, decided not to return to Chile during the criminal process and obtained political asylum in the United States, the only Chilean to attain such status after the dictatorship. Despite repeated calls from the Inter-American Commission on Human Rights and its Special Rapporteur for Freedom of Expression, the Chilean judiciary took no action to amend its decisions in this case.

The censorship of the book and the prosecution of its author produced a widespread reaction in Chile. Even the political class, which not only had supported the legislation until that point, but had also used it (e.g., in the aforementioned Cuadra case), protested these judicial decisions. In the public's opinion, this was an attempt by the judicial branch to cover up its poor record.

This case led to the reform of the State Security Law in April 2001. Article 6.b of the law, which contained a *desacato* provision, was amended, and no longer contains the provision. Another important modification was the derogation of Article 16, which had been used as a basis for censorship in the case of *El Libro Negro de la Justicia Chilena*, as well as others.

However, sending a signal that the judiciary's power to prohibit publications had not disappeared with the reform of the State Security Law, the censorship of Matus' book continued for several months. The basis for censorship became an interpretation of the Criminal Procedural Code, while the judge in charge of the investigation allegedly determined whether the book might violate some norms of the penal code. Finally, the book was released in late 2001.

During the same time the Parliament was discussing the reform of the State Security Law, some organizations from the civil society, a few parliamentarians, and other politicians stated that this was the occasion for the abrogation of all *desacato* laws from the Chilean legal system. However, the Parliament soon discarded this possibility after many of its members said that due to their positions, they need more protection than ordinary citizens. They also said that after the public reaction to the *El Libro Negro* events, it was unforeseeable that remaining *desacato* provisions in the penal code and the Code of Military Justice actually would be enforced. But they were wrong. In December 2001 (a few months after the reform of the State Security Law) those remnants of *desacato* laws were in effect brought to life, when the entire Supreme Court presented a case under a *desacato* regulation contained in the penal code. The case was against television panelist Eduardo Yáñez, who said that the Chilean judiciary was "immoral, coward, and corrupt." Yáñez's remarks were made during a discussion about a case that involved a very serious judicial error, in which the Supreme Court had denied the victim any compensation.[8]

Nine months after the case against Yáñez was initiated and after several public commitments by executive-branch authorities, a draft legislation to derogate all remaining *desacato* laws was introduced to Congress. Later on, the executive branch designated this draft legislation as urgent, a measure within the Chilean legal system that is indispensable to ensure some progress in the process of discussing and eventually enacting a law. However, several months passed and no further initiative was taken. Meanwhile, a lower court ruled that Yáñez was guilty of the alleged crime.

In March 2003 the urgent status of the draft legislation to derogate the *desacato* laws expired, and the executive branch did not reinstate it. However, the draft law received urgent status again in April.

Additionally, in an unexpected development in early April 2003, an appeals court absolved Yáñez, stating that his expressions lacked *animus injuriandi*, which means they were not intended to harm the honor of the Supreme Court justices. This was a brave decision by the Court of Appeals justices, since the case concerned their superiors, who evaluate them annually.

As for prior censorship in connection with the State Security Law, it must be noted that despite the abrogation of Article 16 (upon which the prohibition of *El Libro Negro de la Justicia Chilena* was based), the tribunals could use another provision that remains in Article 30 of the law for the same purpose. This provision is ambiguous, because it does not make clear whether a court has the power to confiscate all issues of a publication or only a few of them.

LEGISLATION TO OBTAIN ACCESS TO INFORMATION

Despite the fact that the Chilean Constitution does not explicitly recognize the right to access information, the Constitutional Court developed some jurisprudence in this regard. However, this jurisprudence does not recognize the population's need to access information kept by the state; rather, it refers to this right as a complement to the media's right to inform the population. Therefore, there has been no judicial action based directly on a constitutional right to access information.

In this context, to start with judicial actions it became a need to first have legislation on this matter. This legislation is the Law on Administrative Probity, enacted in December 1999,[9] which contains several provisions that provide the basis in this respect and create a procedure for such purpose. This law establishes as a general principle that public functions will be accomplished with transparency to ensure that citizens have knowledge about the procedures, content, and other fundamentals of public decisions. It adds that both administrative acts and the documents related to those decisions will be made available to the population. These provisions are also applicable to private enterprises whose work serves a public need and to enterprises in which the state has some participation described in the law.

The Law on Administrative Probity contains five exceptions to the general transparency rule for public decisions and the acts and documents linked to them. One of the exceptions explicitly refers to the nation's security and the national interest. Another exception applies to cases in which the disclosure of the sought-after information could prevent or obstruct the proper functioning of the department from which the information is requested. This provision has been criticized as vague and "likely to be interpreted expansively by officials as a basis for denying information," and thus "difficult to challenge in court."[10] Also, this could become an easier way for organizations whose tasks are related to national security issues to deny information.

In connection to this law, in January 2001, the executive enacted general regulations. According to the Law on Administrative Probity, the regulations were intended to develop the provisions on this matter in more detail. However, the regulations went further, in fact restricting the scope of the principles of transparency and publicity the law established. This was, of course, a violation of the law and of the Constitution. The Law on Administrative Probity requires the regulations to refer to the *documents and background information*; however, the regulations made reference not only to them, but also to the confidentiality and secrecy of the states' and private organizations' *actions.*

The consequences were evident promptly. The Law on Administrative Probity states that all organizations it regulates must enact their own regulations on access to information (based, of course, on the law and the general regulations). A number of these organizations then started to declare many actions confidential or secret, including complaints presented to them, judicial complaints brought by the organizations themselves, and others. This situation has received wide criticism, but thus far it continues to occur as described. On the other hand, some state organizations have implemented more open practices. These disparities show the difficulty inherent in changing work routines in public administration.

When an organ denies access to information, a judicial remedy can be sought. The Law on Administrative Probity establishes a different treatment for cases in which national security is the alleged exception preventing access. For all other exceptions, a district court must solve this matter, and eventually it can reach a Court of Appeals. National security cases, however, must be presented directly to the Supreme Court.

Ever since the law was enacted three years ago, the district courts have developed some interesting, although still incipient, jurisprudence in cases with no connection to national security.[11] To date, no national security cases have been brought before the tribunals based on the Law on Administrative Probity.

Overall, the adoption of the Law on Administrative Probity was a step forward in the process of granting access to information in Chile. The entire picture of its implementation, however, shows there still is a long road that must be followed to make this right fully effective.

As for the Armed Forces' access to information, the Code of Military Justice and a series of regulations contain norms about access to information and restrictions on national security grounds. Article 436 of the Code of Military Justice defines secret documents as those directly related by content to state security, national defense, internal public order, or the security of persons.

Articles 144 and 144 bis of the Code of Military Justice regulate the disclosure of secret documents during judicial investigations. According to Article 144, the military prosecutor in charge of the investigation is the only person who can request the submission of secret documents. In judicial cases in which the prosecutor deems it necessary to request secret documents, he or she must ask the respective commander-in-chief, who can refuse to submit the document on the grounds that it would affect state security, national defense, internal public order, or the security of persons. If the prosecutor believes it is essential to obtain the document, the Supreme Court, in addition to the legal counsel of the Army, decides on the matter.[12] In any event, individuals involved in a judicial investigation conducted by a military prosecutor may not access any secret documents, even if the disclosure of a secret document would be relevant to their defense.

The situation is similar in cases within civilian jurisdiction; the judge in charge of a criminal investigation must request the submission of a secret document to the respective commander-in-chief (Article 53 of the Criminal Procedural Code in connection to articles 144 and 144 bis of the military code).

Additional provisions about the protection of secrecy within the Armed

Forces are established in the Regulations on Intelligence and Military Security. According to these regulations, as a general rule, all matters concerning the Armed Forces are public. They add, however, that such matters become classified when their disclosure would actually or potentially harm the army or the state, either within the country or abroad. These provisions usually have been construed as establishing a sort of objective responsibility, that is, a person will be considered responsible solely on the basis of having had knowledge of a classified document without the power or the authorization to do so.

These regulations contain detailed provisions about the formalities required to gain access to secret documents. To obtain and to handle classified information, a member of the military must have authorization, which he receives with a degree of access (*grado de acceso*). The type of classified documents he can examine depends on the degree of access he is granted.

The Administrative Regulations on Correspondence and Documentation go further by classifying the potential harm that unpermitted disclosures cause and by ruling on degrees of secrecy. In addition, there are regulations on secrecy about matters related to the Armed Forces that are applicable to former military officers as well. This is the case of the Regulations of the Garrison Service of the Army.

In connection with this matter, a book entitled *Ethics and Intelligence Services* (*Ética y Servicios de Inteligencia*) has been banned in Chile for 10 years now. In 1993, Humberto Palamara, a former intelligence officer with the Navy, attempted to publish this book, but the military courts decided he could not. Palamara already was retired and was only under contract with the Navy when he wrote the book. *Ethics and Intelligence Services* provided no accounts of the Navy's internal regulations or practices; instead, the book focused on developing some standards that, according to its author, should be the basis for future work in this area, in order to avoid repetition of the kinds of widespread abuses the Intelligence Services committed during the dictatorship. Although Navy authorities did not state it explicitly, what might have aroused some suspicions about Palamara's book was the fact that it particularly stressed the necessity of keeping intelligence activities in accordance with human rights standards, opposing torture and stating that it is not the role of intelligence services to detain or interrogate persons.[13]

A military court prohibited the book even before it was published. To enforce its decision, the court searched both the printing facilities where the publication was in process and Palamara's house. Despite the fact that the ban was supposed to be temporary, the military personnel who searched the house not only confiscated the copies of the book they found there, but also deleted the text from the hard disk of Palamara's computer.

Some time later, the court ordered two experts to review the book to find out whether it threatened national security. It was very striking when the military experts who reviewed the book at the tribunal's request concluded that it contained no confidential information or analysis affecting national security or defense. Still, the book was not released. Instead, two additional military experts were appointed, and they concluded that the book affected the Navy's institutional interests. However, they did not report that the Navy might be harmed as a result of its publication. The experts affirmed their conclusion about the book's effects on the Navy's institutional interests by saying, "in his (Palamara's) statement that his piece responds 'to the moral obligation that a person has to disseminate his knowledge and experiences to others,' it is implicit that the author's capacity to write on the topic is based on his Navy training as an intelligence specialist."

Palamara was charged with two criminal offenses. The first was for attempting to publish the book without the Navy's authorization, causing danger to national security. The second was for disobedience, for not giving the book to Navy authorities when he was ordered to do so. The case went through three courts: first, to a military tribunal; second, to a martial court, which operates as an appellate court within the military jurisdiction and has a mixed civilian/military composition (three military justices and two civilians); and finally to the Supreme Court, where an Armed Forces representative is added to the panel of five Supreme Court justices for cases under military jurisdiction.

On the first charge, Palamara's failure to request authorization was considered to be a violation of the Ordinance of the Navy of Chile, which states in Article 89:

> It is forbidden to all members of the Navy or persons in its service to publish or to facilitate the publication in the press of articles involving criticism of the Navy services, of other armed institutions, of public organizations, or of the government.
>
> It is likewise forbidden to publish, directly or indirectly, articles concerning matters of a secret or confidential nature, matters of a political or religious nature, as well as others that could lead to controversies in which the good name of the Navy could be involved.
>
> Taking into account the above mentioned restrictions, Navy personnel can make publications in the press, in their personal capacity, with the prior knowledge and authorization of his/her Commandant or the Competent Navy Authority.
>
> In times of war or when circumstances so require, the Commander in Chief of the Navy can suspend or limit this authorization.[14]

The judicial decision on Palamara's disobedience charge was based in Article 337.3 of the military code. The grounds of the charge were that Palamara had been forbidden to give any information to the press, but he did, despite the prohibition. In his response to the charges against him, Palamara disputed the facts and the military jurisdiction over his case. However, military jurisdiction is typical in Chile for this type of case, so it was not unexpected that the military tribunal would retain its jurisdiction, which it did.

Palamara was convicted to two suspended sentences, each of them for 61 days. In addition, he was condemned to an accessory penalty of confiscation of his book.

In the second court process, Palamara was convicted for libel (*desacato*) against the Navy prosecutor and sentenced to 61 days of imprisonment. This was a consequence of some statements Palamara made to the press after his book was confiscated, which the prosecutor ordered. Palamara said, "there are reasons to assume that the Office of the Navy Prosecutor (*Fiscalía Naval*) forged legal documents and lied to the Court of Appeals when consulted about who had made the complaint that initiated the summary process as well as about the case number...."[15]

The first court, the military tribunal, had absolved Palamara of the libel charge because his statement did not refer to the Navy prosecutor (*Fiscal Naval*) nor to any individual, but to the Office of the Navy Prosecutor (*Fiscalía Naval*), thus lacking a key element of libel. A divided decision by the martial court reversed the decision and sentenced Palamara to 61 days in prison. Finally, the Supreme Court, in another divided decision, confirmed the martial court's condemnatory decision.

Palamara later brought a complaint against Chile before the Inter-American Commission on Human Rights for violation of Article 13 of the American Convention, which protects freedom of expression and contains other articles that guarantee due process of law. The commission, however, has proceeded with the case at a very slow pace. After several years, it finally declared the case admissible in 2001 and is currently moving to reach a final decision. Meanwhile, Palamara's book remains banned from publication.

THE DEBATE ABOUT THE CREATION OF A NATIONAL INTELLIGENCE AGENCY

Two intelligence agencies committed the most significant human rights violations in Chile during the dictatorship. They were the National Directorate on Intelligence (DINA, by its Spanish acronym) and the National Intelligence Central (CNI). The first operated from 1973 to 1977, perpetrating the vast majority of extrajudicial executions, forced disappearances, and torture during that period. The second functioned from 1977 until the end of the military regime in 1990, committing torture and other crimes on a massive, systematic basis.

In addition to the crimes they committed, these agencies from the dictatorship strengthened a culture of secrecy and misinformation. In fact, the very creation of the DINA was done through a secret act, which was not published in the *Official Bulletin* (*Diario Oficial*) as it should have been. The DINA was involved in several cases of disseminating misinformation, the most notorious of which was its edition of a fake newspaper in Brazil that stated that 119 people whose disappearance Chilean NGOs had denounced had died abroad as part of guerrilla actions. Chilean newspapers later widely reproduced this false information.[16] As for the CNI, during the 1980s when massive demonstrations against the dictatorship took

place regularly, it developed strategies to distract the public from the country's political and economic problems. Its most famous distraction was a series of fake apparitions of the Virgin Mary, which the Catholic Church dismissed.

When the transition to democracy began and the CNI was abolished, it was not replaced. However, the Intelligence Services of the Armed Forces continued its operations – the Directorate of Intelligence of the Army (DINE) being the one with the highest profile – and that agency hired many former members of the CNI. In the '90s, the DINE was involved in a surveillance operation to prevent Sebastián Piñera, a moderate right-wing candidate who had opposed Pinochet, from running for president of Chile. A DINE officer taped a phone conversation during which Piñera discussed plans to harass the other potential right-wing candidate, and then managed to have the tape released on television, prompting Piñera to withdraw from the presidential race. This opened the way for a third candidate from the right – a candidate who was closer to the military – to run for the presidency.

Another factor that was considered in this respect during the first years of the transition was the persistence of some armed groups that had fought against the dictatorship. The most significant of them, the Frente Patriótico Manuel Rodríguez (FPMR), split up; one of its factions joined the Communist Party and left behind its weapons, and the other group continued with the old method. In addition, the Movimiento Lautaro, a group that had adopted what were almost anarchist ideas, remained active.

The government decided not to create a special intelligence agency to dismantle these organizations. It did establish an apparatus inside the Ministry of Interior that became controversial because of the methods it used to deal with this problem. By the mid-1990s, the Movimiento Lautaro had been dismantled, and the FPMR was virtually in the same situation.

Since then, however, the idea of establishing a national intelligence agency has arisen from time to time. This became more concrete when the Lagos Administration presented to Congress a draft legislation to establish a National Intelligence Agency (ANI, by its Spanish acronym), and a National Intelligence System, that would comprise that agency and the intelligence offices from the Armed Forces and the police. This draft law is currently under debate in Congress.

According to this draft law, the National Intelligence Agency would be responsible for producing information to help the president of the republic accomplish his/her tasks regarding terrorism, transnational organized crime, and counterintelligence. All of the information this organization gathered would be considered secret, notwithstanding the powers of the Chamber of Deputies, the Senate, the judiciary, and the attorney general's office to request it when necessary. No term has been established for declassifying this information.

THE NATIONAL SECURITY COUNCIL

The Constitution of 1980 created a National Security Council, an institution with no precedent in Chile. This is an organization of mixed military-civilian membership whose reputed goal is to protect national security. Originally, the militaries (including the police) had the majority of the seats in the council. Later on, through a reform introduced to the Constitution, the number of civilian and military members became equal. The Armed Forces still have a strong presence, as each division is represented by its respective commander-in-chief. On the civilian side, the President of the Republic, the Senate, and the Supreme Court and the chief of the office that reviews the legality of executive decrees also are members of this council. A controversial aspect of the National Security Council is the fact that any two of its members can convene it to meet, which gives the Armed Forces the ability to intervene in a field in which civilian authorities should have the initiative in a democratic regime. This council can also influence other institutions; its most outrageous power allows it to nominate two members of the Constitutional Court.

The National Security Council was a consequence of the so-called "national security doctrine." The concept behind the doctrine was that of a *democracia protegida* ("protected democracy"), that is, a political system that should be well aware of actual and potential attempts to destabilize it. To achieve this purpose, it was believed that the Armed Forces should have a permanent presence at the levels at which decisions sensitive to national security are made. This is consistent with the role the Constitution of 1980 assigned to the Armed Forces, to be the guarantors of the Chilean institutionality. At the same time, it is a departure from the prior Constitution of 1925, which established the non-deliberative nature of the Armed Forces. During the transition to a democracy, some initiatives have been taken to

eliminate this council, but to no avail, as members of Congress who are former supporters of the dictatorship effectively have opposed a constitutional reform in this respect. The National Security Council's role became more prominent and visible to the public opinion during Pinochet's detention in London between October 1998 and March 2000, when the commanders in chief asked the council to meet on several occasions and the civilian authorities did not have the power to veto this citation. It had three meetings in connection with Pinochet's detention and an additional meeting when he was formally accused by a Chilean judge in 2001.

After the Pinochet detention and his final release by the Chilean Courts based on mental health grounds, the Armed Forces modified some of their procedures, including how they adopt policies and making public statements more coherent with its reputed role in a democratic system. In fact, they even changed their attitude toward the prosecution and sanction of current and former members who perpetrated gross violations in the past; the Armed Forces, as a general statement, no longer are posing obstacles to judicial investigations. In this context, the existence of a National Security Council with its current powers represents an anomaly.

STATES OF EXCEPTION

In its original text, the Constitution currently in force (enacted by the dictatorship in 1980) contravened international human rights standards in several ways in its States of Exception. Although the Constitution has been reformed in this area over the years, it is still inconsistent with some international standards. Despite the fact that, as stated in the first section of this paper, the Constitution established a state duty to respect such standards, no amendments have been introduced, nor has jurisprudence been developed to overcome these problems.

The first aspect of the Constitution that reveals inconsistencies concerns the reasons for declaring a State of Exception. The International Covenant on Civil and Political Rights, to which Chile is a party, provides in Article 4 that in order to declare a State of Exception that restricts rights such as freedom of expression (including access to information), the subject at hand must pose a threat to the nation. In the Chilean Constitution, however, the three kinds of States of Exception that allow restrictions of freedom of

expression do not mention a threat to the nation. Although some reasons established in the domestic regulation of States of Exception, such as war, can represent threats under certain circumstances, others cannot. It seems that internal commotion (based on which Chile can declare a State of Siege) and public calamity (upon which a State of Catastrophe can be declared) do not threaten the nation's life.

The second inconsistency involves the role of the tribunals during States of Exception. This is a matter of utmost importance in Chile, where historically, the judiciary has not made significant efforts to control executive-branch actions regarding States of Exception, thus opening the way for the executive to commit grave human rights violations by citing the alleged goal of protecting national security. According to international law, the fact that States of Exception allow the restriction of rights such as freedom of expression and access to information does not imply that the executive branch can exercise its expanded powers in an arbitrary manner or without control. The International Covenant on Civil and Political Rights states that the government must take measures "to the extent strictly required by the exigencies of the situation;" that is, the tribunals must analyze the circumstances surrounding such measures. In addition, the Inter-American Court of Human Rights has been very precise in this respect, stating that according to international law, the judiciary must retain its powers to control the executive-branch actions both at the formal and substantial levels. This means that the tribunals must determine whether an executive action actually was intended to satisfy its alleged goal (i.e., to protect national security) and was suitable for that purpose, and they must establish whether the measure was proportional to the circumstances.

The Chilean Constitution, though, provides that judicial control in these situations must be merely formal; that is, it must be confined to determining whether the competent executive organization made the decision and whether it followed the formal steps (i.e., the issuing of a decree). The Constitution explicitly prohibits judicial intervention at the level of substantial control, which is inconsistent with international law. According to Article 41.3 of the Constitution, the courts are banned from analyzing either the fundamentals of or the circumstances under which political authorities adopt their restrictive measures.

The fact that during the transition Chile has declared no States of

Exception has put these problems on the back burner of the public agenda, and no serious efforts have been made to amend this situation that could have grave consequences if circumstances change.

CONCLUSION

As in the rest of Latin America, in Chile the concept of national security has been pervaded by authoritarian features that stem from its days as a Spanish colony. This means the law deems that public authorities deserve a higher status than regular citizens, and that their honor is a matter of state security. It also implies that transparency and accountability are not clearly defined as central features of the political system. These trends were brought to an extreme under the influence of the so-called "national security doctrine," as developed and disseminated by The School of the Americas and other U.S. institutions during the Cold War.

Thirteen years after the end of the Pinochet regime, the effects of the "national security doctrine" have dissipated to a large extent. In Chile, however, the role of the National Security Council, together with other characteristics of the country's political system, demonstrate that some effects still exist.

It is more difficult to modify the older authoritarian trends that pervade the Chilean culture, politics, and legal system. While several legal reforms have taken place during the transition to expand access to information and make the concept of national security more compatible with a democratic system, the task is far from complete. A series of legal obstacles have not been removed yet, and many judges do not apply provisions related to national security and access to information in a manner consistent with international human rights standards and with fundamental rights enshrined in the Constitution.

NOTES

[1] The author thanks Domingo Lovera for his research assistance.

[2] Constitutional Court of Chile, Judgment #226, Oct. 30, 1995. Translation by the author.

[3] For further analysis, see González, Felipe, Jorge Mera, and Juan Enrique Vargas. 1991. *Protección Democrática de la Seguridad del Estado.*

[4] *Against José Antonio Gómez*, Revista de Derecho y Jurisprudencia, T.LXIX, 2ª p., Secc. 4ª, pp. 4 ss. José Antonio Gómez was the director of the leftist newspaper *Puro Chile*. The process against him took place prior to the military regime. This jurisprudence has been reaffirmed on many occasions.

[5] See Human Rights Watch. 1998. *Los Límites de la Tolerancia: Libertad de Expresión y Debate Público en Chile*; p. 167. See also, González, Felipe. 2000. "Leyes de Desacato y Libertad de Expresión." In *Igualdad, Libertad de Expresión e Interés Público*, edited by Felipe González and Felipe Viveros; pp. 219-263, at 234. The State Security Law has also been applied in connection with other matters, e.g., in the context of relations between indigenous groups and the state in Southern Chile.

[6] Senator José Antonio Viera-Gallo, a member of the Socialist Party, was accused under the State Security Law by then-Army Commander-in-Chief and former dictator General Augusto Pinochet. In a TV program, Viera-Gallo said in the context of a live discussion on corruption that during his government, Gen. Pinochet "put his hands" (*metió las manos*). Gen. Pinochet interpreted the statement as an accusation of corruption. The judicial proceedings were quickly closed after Viera-Gallo publicly apologized, stating that it was not his intention to accuse Gen. Pinochet. As a result of this incident, Viera-Gallo changed his opinion about the State Security Law, saying it should be derogated.

Another well publicized case was that against Arturo Barrios, who was president of the Youth of the Socialist Party at the time. Barrios said that Gen. Pinochet was an assassin. He was convicted to a 541-day suspended sentence for disturbing the public order under the State Security Law.

In a very similar case, Gen. Pinochet accused Gladys Marín, then secretary general of the Communist Party, of disturbing the public order under the State Security Law for calling him an assassin. After governmental authorities intervened, however, Gen. Pinochet withdrew the charges.

A fourth case Gen. Pinochet presented on state security grounds was against Nolberto Díaz, then president of the Youth of the Christian Democratic Party. The charges were dismissed. In a broadcasting program in 1996, Díaz stated that, "they want us [the youngsters] to serve at the draft having the same elderly, former dictator, as the commander-in-chief of the Armed Forces." He also said that he thought links existed between Chilean army officers and the killing of a former Chilean intelligence officer that occurred in Uruguay, asking about the purpose of a trip Gen. Pinochet made to Uruguay when a judicial investigation was being carried out. The judge presiding over the case against Díaz closed the case until sufficient proof could be provided. The Court of Appeals confirmed this decision, and the Supreme Court refused to review the case arguing lack of jurisdiction in late 1996. The case was never reopened.

[7] Cuadra was a former minister of the military regime who publicly stated that there were members of Congress who used cocaine but refused to identify them. The House of Representatives and the Senate, following almost unanimous agreements, accused Cuadra of violating the State Security Law. In the first instance, Cuadra was condemned to a suspended sentence for disturbing the public order. The Court of Appeals later revoked this decision, declaring that Cuadra's statements did not affect the public order in any way. The decision quoted Minister of Interior Carlos Figueroa, who said to the press before Cuadra was charged that public order was not affected. His opinion was relevant, because the minister of interior is the authority whose role is to protect public order. The Court of Appeals' decision should have been definitive, because Congress recently had passed legislation restricting access to the Supreme Court in order to reduce its docket of cases, and the Supreme Court should not review cases like Cuadra's. However, the very same parliamentaries who had passed that legislation presented the Cuadra case before the Supreme Court. (The Court found a very particular ground to reaffirm its jurisdiction over the case, stating that the legislation restricting its powers was partially unconstitutional. It was unprecedented for the Supreme Court to declare a law unconstitutional without a prior request by the complainant, as the Court did in this case. Of course, the parliamentaries could not make such petition of unconstitutionality, since they had just approved the legislation.) Finally in 1996, the Supreme Court condemned Cuadra for an offense against public order, based on the doctrine that it is beyond the Court's powers to determine whether or not public order has, in fact, been affected.

[8] See Facultad de Derecho Universidad Diego Portales. 2003. *Informe Anual Sobre Derechos Humanos en Chile 2003* (Facts of 2002); pp. 221 and 222.

[9] Ley 19.653, Dec. 14, 1999.

[10] Human Rights Watch. 2001. Pr*ogress Stalled: Setbacks in Freedom of Expression Reform*; p. 41.

[11] See Facultad de Derecho Universidad Diego Portales, p. 231.

12 According to Article 70-A of the military code, in cases under military jurisdiction, the Legal Counsel of the Army integrates the Supreme Court, regardless of the presence of militaries or civilians among the parties to the process.

[13] While Palamara has never openly criticized intelligence activities undertaken during the military regime, in broadcast appearances he has kept his distance from the intelligence agencies' role during those years, recognizing the Truth Commission Report as a valuable source of information (the Navy, on the contrary, publicly criticized this report).

[14] The original in Spanish reads as follows:

Estará prohibido a todo miembro de la Armada o persona que se encuentre a su servicio, publicar o dar facilidades para que se publiquen en la prensa, artículos que envuelvan una crítica a los servicios de la Armada, de otra institución armada, de organismos públicos o de gobierno.

Igualmente estará prohibido publicar, directa o indirectamente, artículos que se refieran a asuntos de carácter secreto, reservado o confidencial, temas políticos o religiosos u otros que puedan dar margen a una polémica o controversia en la cual se pueda ver envuelto el buen nombre de la institución.

Teniendo en cuenta las anteriores restricciones, el personal de la Armada podrá hacer publicaciones a la prensa, a título personal, previo conocimiento y autorización de su Comandante o de la Autoridad Naval competente.

En tiempo de guerra o cuando las circunstancias así lo exijan, la Comandancia en Jefe de la Armada podrá suspender o limitar esta autorización.

[15] *La Prensa Austral*. May 7, 1993.

[16] See CODEPU-DIT-T. 1994. *La Gran Mentira: El Caso de las ´Listas de los* 119.

ACCESS TO INFORMATION AND NATIONAL SECURITY IN SOUTH AFRICA

Jonathan Klaaren, Professor and Co-Director
Research Unit on Law & Administration
University of Witwatersrand

INTRODUCTION: THE PROMOTION AND THE PROTECTION OF INFORMATION[1]

The two South African statutes most relevant to national security information have similar titles but essentially approach the issue from opposite perspectives. The Promotion of Access to Information Act and the Protection of Information Act also come from two different eras in South Africa national history.

South Africa's constitutional right of access to information is implemented through the Promotion of Access to Information Act 2 of 2000 (AIA). This legislation gives effect to and is itself mandated by the post-apartheid Constitution, generally acknowledged as globally progressive. In one of the legislation's innovations, the AIA extends the gambit of right to information to the private sector. The AIA was enacted in 2000 and has fully taken effect, although some of its compliance deadlines have been extended.[2]

The national security ground of refusal to access to information is contained in section 41 of the AIA.[3] That section protects information the disclosure of which could reasonably be expected to cause prejudice to defense, security, or international relations. It also protects information required to be held in confidence due to an international agreement or supplied by another state in confidence. The ground is discretionary

and may be waived. In the South African transition, an early and significant judicial commission of inquiry established the principle that foreign policy embarrassment is an insufficient reason for non-disclosure of military information.[4]

This paper will not focus either on the AIA generally or on the outlines of section 41 specifically. Instead, the most significant feature of the AIA with respect to national security information in South Africa is not what the AIA does but rather what the AIA does not do. The AIA does not repeal pre-existing government secrecy and confidentiality laws. Even after the enactment of the AIA, the disclosure of the information through any means other than in response to a formal access to information request remains subject to law and regulations preserving confidentiality in government. These laws and regulations include the Protection of Information Act of 1982. The AIA does not strike down those laws and regulations. This is the case even though the AIA does apply to their exclusion in respect of formal AIA requests for records.[5] These laws and regulations restricting the disclosure of information by current and former public officials of course remain subject to the constitutional rights of access to information and freedom of expression.

The current centerpiece of South African legislation restricting disclosure of information is the Protection of Information Act 84 of 1982. This Act replaced the Official Secrets Act 16 of 1956. The Protection of Information Act is very broad in its pursuit of government secrecy. A look at the wording of section 4 of the Protection of Information Act illustrates its breadth. Subsection 4(1)(b) targets 'any person who has in his possession or under his control or at his disposal ... any document, model, article or information ... which has been entrusted in confidence to him by any person holding office under the Government ... or which he has obtained or to which he has had access to by virtue of his position as a person who holds *or has held office* [or a contract] under the Government...and the secrecy of which...he knows or reasonably should know to be required by the security *or other interests* of the Republic' [emphasis added].[6] This subsection prohibits the disclosing of the information to a non-authorized person as well as failing to take care of such information. The following subsection prohibits the receiving of such a document. Section 4 thus makes little or no distinction between information that should not be disclosed because of its military or national security significance and other information held by the public service

that should not be disclosed. Furthermore, section 4 makes no distinction in its application to current and former public officials. The extent of application of section 4 has real consequences: a violation of section 4(1) is made an offense punishable by up to 10 years imprisonment and a fine.

Other sections of the Protection of Information Act appear to be more narrowly intended for national security or military use.[7] For instance, section 3 contains a prohibition in 3(a) on obtaining information "used, kept, made or obtained" in any prohibited "place," which is primarily defined to include defense works and armaments production facilities. Section 3(b) also prohibits the preparation or compilation of a document relating to the "defense of the Republic, any military matter, any security matter or the prevention or combating of terrorism". Both of these actions are criminalized and there is a purposive requirement to both.

Without engaging in a detailed or comprehensive examination of section 3 of the Protection of Information Act and section 41 of the Promotion of Access to Information Act, it is clear that the AIA takes a detailed and particularized approach to the determination of legitimate disclosure of military information. This can be contrasted to the more categorical approach of the Protection of Information Act. While the AIA does include a categorical subsection, it also gives examples of what will fit within that category. On the whole, the AIA approach is less susceptible to expansion.

IMPLEMENTATION OF THE PROTECTION OF INFORMATION ACT: THE MINIMUM INFORMATION SECURITY STANDARDS (MISS)

Of course, it is not enough to look at the law on the books. One must examine the law as it is implemented. The principal mechanism by which the Protection of Information Act is currently implemented is a Cabinet-level policy document. This is the document on Minimum Information Security Standards (MISS). The Minimum Information Security Standards document was approved by Cabinet on 4 December 1996 as "national information security policy" and has not been updated. As policy, the MISS is to be implemented by each public institution as

well as by some private institutions working with public ones. According to its preface, the MISS "must be maintained by all institutions who handle sensitive/classified material of the Republic." Each institution is to compile its own rules of procedure using the MISS policy as a set of minimum standards.[8]

Despite the department-level application of the MISS policy, the leading role in the implementation of the MISS is taken by the National Intelligence Agency. The NIA is one of the several security institutions set up by the South African Constitution and legislation. It is subject to special procedures of Parliamentary accountability. NIA security advisers are available to advise public institutions on MISS implementation.[9] Moreover, the NIA is responsible for issuing amendments to the MISS.[10] As a general policy applicable to all government departments, this aspect of the implementation of the MISS can draw only upon the force of section 4 of the Protection of Information Act.

It is important to realize that a separate specific policy governs information security within the South African defense community. This more narrow military information security policy is contained in a set of South African National defense Force Orders (SANDF/INT DIV/2/97). This policy applies principally to the SANDF and Armscor.[11] Furthermore, another set of separate policies govern the South African Police Service and the South African Secret Service.[12] The implementation of information security within the security services could draw upon the force of all sections of the Protection of Information Act and not merely section 4.

What is also crucial to realize is that the information covered by the SANDF Order is much narrower than the information covered by the MISS. Indeed, the SANDF policy would appear to be both narrower in application and more broadly supported in law than the MISS itself. Essentially, the SANDF policy covers only military or traditional national security information. It is not through its application provisions but rather through its content definition that the scope of the SANDF Order is restricted. In other words, it is the kind of information and not the kind of public body that limits the operation and coverage of the SANDF Order. In the SANDF Order, "classified information" is defined as:

> any information or material which is held by or for, is produced in or for, or is under the control of the State or which concerns the State and which for the sake of national security be exempted from disclosure and must enjoy protection against compromise. Such information is classified either Restricted, Confidential, Secret, or Top Secret according to the degree of damage the State may suffer as a consequence of its unauthorized disclosure.[13]

From the point of view of history and bureaucratic policy development, it seems obvious that the MISS is based upon a military/national security information classification scheme roughly similar to that one presently contained in the SANDF Order.[14] In other words, the MISS is more or less a cut and paste from an earlier version of the SANDF order. Presumably, this occurred at some point in the 1980s when the national security state was ascendant and the influence of the South African military was at its peak.[15]

This brings about a significant difference that opens the MISS to constitutional challenge. The meaning of the term "classified" in the MISS is much broader than the term "classified" in the SANDF Order. Classified no longer has the substantive meaning of national security. Instead, in the MISS it means:

> Sensitive information which, in the national interest, is held by, is produced in or is under the control of the State or which concerns the State and which must by reasons of its sensitive nature, be exempted from disclosure and must enjoy protection against compromise.[16]

This history contributes to the overbreadth of the MISS. In essence, the MISS definition of classified information has the shell of the military definition but with its heart — the reference to national security — cut out. The term "sensitive" has replaced "national security." The result is circular. Instead of a substantive, military-based reason for non-disclosure, we have the general reference to "sensitive information ... which by reasons of its sensitive nature [must] be exempted from disclosure." Interpreting the MISS most broadly, a military information security policy has been crudely and inappropriately adapted to attempt to cover the entire public sector. While this can and has been argued to be justified along the lines of how economic espionage has replaced military espionage in the new global economy, it is nonetheless a far cry from the traditional definition of national security.[17]

Dating from what must be a history subsequent to the one just described, the MISS also shows internal evidence of its conflict with the constitutional right of access to information. Together with the preface, the use of the phrase "must be exempted from disclosure" in the MISS definition of classified information shows that the MISS in its post-apartheid version was revised within the legal context of the right to information. Read in context with the preface of the MISS, it is clear that this phrase derives directly from the policy proposals and from the draft Open Democracy Bill (the precursor to the Promotion of Access to Information Act).[18] Indeed, the MISS itself foregrounds its allegiance to the AIA in the preface: "Our need for secrecy and therefore information security measures in a democratic and open society with transparency in its government administration according to the policy proposals regarding the intended Open Democracy Act have been taken into account." This reference to the policy of the Promotion of Access to Information Act becomes even more specific in Chapter 1 of the MISS:

> Although exemptions will have to be restricted to the minimum (according to the policy proposals regarding the intended Open Democracy Act), that category of information which will be exempted, will as such need protection. The mere fact that information is exempted from disclosure in terms of the Open Democracy Act, does not provide it with sufficient protection. ... *Where information is exempted from disclosure*, it implies that security measures will apply in full. This document is aimed at exactly that need: providing the necessary procedures and measures to protect such information. *It is clear that security measures do not concern all information* and are therefore not contrary to transparency, but indeed necessary for responsible governance.[19]

One could even argue to a court that these references by the MISS to the AIA mean that properly (and narrowly) interpreted there should be no conflict between the substantive information disclosure policy of the Promotion of Access to Information Act and the substantive information disclosure policy of the MISS. Since the MISS itself claims to be within the spirit of the AIA, the AIA should clearly trump the MISS.[20]

PRACTICES OF THE MISS: SECURITY CLEARANCE AND INSTITUTIONAL PROCEDURES

That benevolent interpretation has not been the one put into practice. As one might expect of an apartheid era information policy, the spirit of the MISS and in particular its security screening procedures run almost directly counter to the spirit and purpose as well as the procedures and institutions of the Promotion of Access to Information Act. In practice, the MISS is a de facto government general confidentiality policy. The remainder of this section describes the information security implementation procedures of the MISS: a security clearance procedure and a procedure for signing declarations as well as monitoring by the NIA.

The main feature of the implementation of the MISS is a security clearance procedure.[21] With respect to governmental and parastatal personnel, the investigation phase of the security clearance process is conducted by the Crime Combating and Investigation Division of the South African Police Service.[22] In order to obtain a security clearance, a public service employee must complete a 9-page Security Clearance Form (Z204).[23] It may be that interviews are conducted in some cases.[24] SAPS will then recommend security clearance. The actual decision-making is the responsibility of each institution.[25]

While the institutional centerpiece of the MISS is this security clearance procedure, it is clear that monitoring of the procedure by the NIA is a significant feature. As the implementor of the MISS and the agency charged with the defensive aspect of counter-intelligence (e.g. information security), the security clearance process implementing the MISS is coordinated and monitored by the National Intelligence Agency. As such the NIA is tightly linked to the operation and continual monitoring of the security clearance and information security procedures. For instance, in an apparently standard letter granting security clearance, heads of directorates are requested to "see to it" that the person's behavior (once granted a security clearance) is irreproachable. Further, "any breach in security, disembodiment of security measures or risky security behavior must immediately be reported to the Direction: Administration [NIA], so that the situation can be investigated".

In addition to the security clearance procedure (but possibly linked to

that procedure in practice), Appendix B of the MISS contains a standard form for a declaration relating to the Protection of Information Act. The declaration states that the signatory is familiar with the Protection of Information Act and more particularly with section 4. A signatory of a declaration might be presumed to have read the provisions of section 4 which are printed on the back of the form. The declaration goes to state:

> I realize that I am guilty of an offense should I disclose any information I have at my disposal on account of my office and in respect of which I know, or should reasonably know, that the security of other interests of the Republic demands that such information be kept secret, to anyone other than a person lawfully entitled to it; or a person to whom I am in duty bound to disclose it in the interests of the Republic; or a person to whom I have been authorized to disclose such information either by the Head of Department or another officials authorized by him.

Furthermore, the declaration states "I realize that the above provisions and instructions are not applicable during my term of office only, but also after my services in the Department have been terminated".

There is no apparent express authority in the Protection of Information Act for these declarations. In at least some departments, the declaration may be required as part of the security clearance process.[26] Technically, the declarations do not add any legal force to the prohibition against disclosure of information contained in the Act itself. Nonetheless, they presumably would aid the State in a prosecution in terms of the Act. The signed declarations would assist in demonstrating that an accused knew or reasonably should have known about the terms of section 4's prohibition on disclosure.

CONSTITUTIONAL PROSPECTS OF THE PROTECTION OF INFORMATION ACT AND THE MISS

As I have argued more fully elsewhere, the security clearance, NIA monitoring, and declaration signing procedures of the MISS clearly inhibit and endanger the South African constitutional rights of access to

information (s 32) and freedom of expression (s 16).[27] In addition to the direct application of these constitutional rights, the South African Constitutional Court has made it clear that where administrative discretion may impinge upon these rights, Parliament must be careful to provide clear guidelines for the exercise of such administrative discretion.[28] Where no such guidelines are provided by Parliament, the section enabling such administrative discretion is more likely to be found to be unconstitutional.

One important case decided in the Southern African context supports the argument for partial unconstitutionality of the Protection of Information Act.[29] In a case reported in 1996, *Kauesa v Minister of Home Affairs*, the Supreme Court of Namibia invalidated a regulation which made it an offense for a member of the police force to comment "unfavourably in public upon the administration of the force or any other Government Department." The unfavorable comment at issue in the case was a comment on affirmative action in the Namibian police force. The court balanced the interest of the citizen member of the police force in expression with that of the state in maintaining discipline, efficiency and obedience in the police force. The regulation was determined to be unconstitutional and not justifiable because it was vague and overbroad and because it was not proportional to its objective.

In particular, the portion of the MISS policy implementing information security beyond the security institutions (e.g. in public institutions beyond NIA, SASS, SAPS, and SANDF) is arguably unconstitutional in its effect. The National Intelligence Agency and other public bodies are likely to run into serious trouble enforcing section 4 of the Protection of Information Act through the MISS. Section 4 is likely to be unconstitutional on its face either as vague and overbroad[30] or as a direct infringement of the constitutional right of freedom of expression (perhaps read with access to information) or as a combination of its breadth and its restriction on fundamental rights.[31] Unless the scope of the MISS is restrictively interpreted in line with the AIA, the same unconstitutional fate awaits its provisions. In any case, the finding of unconstitutionality must apply with even greater force to the system of security clearances, NIA monitoring and Appendix B declarations of the information security policy that the Minimum Information Security Standards document sets out to be national policy. To the extent that

they are applied beyond the realm of the security services as identified in Chapter 11 of the Constitution, these mechanisms are likely to be overbroad and to illegitimately restrict at least the right of freedom of expression.

RECENT ACCESS EVENTS

Two recent events demonstrate the possibilities and tensions for access to information within this framework.[32] The lengthy delay preceding the recent release of the TRC sensitive records demonstrates the continuing power of the intelligence community. Additionally, an analysis of the recent court decision in the C2I2 case also points to the contested understanding of national security information disclosure.

The Sensitive TRC Files[33]

A long saga has surrounded 34 boxes of "sensitive" TRC records removed from the Truth and Reconciliation Commission (TRC) offices in 1999 and placed in the custody of the Department of Justice (DOJ). These records were the ones judged (although the criteria and authority are unclear) most sensitive of those collected by the Truth and Reconciliation Commission. Using the AIA, a South African non-governmental organization, the South African History Archive (SAHA) secured a list of the files in those 34 boxes. The files include a list of informers and a confidential submission by the African National Congress (ANC). The concern of some professional archivists, including SAHA, was for the safekeeping of these records and the potential undue influence over and access to those records that might be exercised by the intelligence community.

This concern appears to have been well-founded since the actual custody of the Department of Justice of these 34 boxes over the past few years has never been clear. In May 2001 SAHA put in an AIA access request to the Department of Justice in relation to these records. In December 2001, DOJ indicated that they did not have the records and suggested that SAHA approach the National Archives. SAHA immediately requested clarification in writing from both the National Archives and the National Intelligence Agency (NIA). National Archives did not respond. In contrast, NIA indicated in writing that the records, to their knowledge, were still in the safe custody of DOJ.

During the second week of April 2002, John Perlman of the radio station SAFM ("the station for the well-informed") conducted a series of interviews with key roleplayers in relation to these "sensitive" TRC records. On 9 April the spokesperson for DOJ informed him that the records were with NIA for safekeeping. And on 12 April the NIA spokesperson stated that the records were indeed with NIA, but emphasized that they would be returned to DOJ shortly.

The CCII case and the Arms Deal

In the late 1990s, South Africa made a large purchase of arms from overseas. This complex set of agreements has been known as the arms deal. The arms deal has generated a number of allegations of corruption and mismanagement. The South African government has investigated some of these instances, but has largely continued to claim that the arms deal was largely free of improprieties. A disappointed tenderer, Richard Young, has used the AIA to attempt to access information relating to the decision not to award his company, CCII, with a contract as well information relating to the government investigation of the arms deal. The government agency primarily involved has been the Auditor General rather than the Minister of Defense. The request for access to information eventually landed in court and resulted in the first significant judicial decision on the AIA.[34] The result was essentially a victory for requesters.[35] The government was ordered to provide a list of documents available and to justify the documents that were not available. The government initially appealed the court's decision to a higher court. However, in March 2003, the Auditor-General withdrew his appeal of the decision and agreed to apply the provisions of the AIA and to hand over the documents that were not protected from disclosure.

WHERE TO FROM HERE (SOUTH AFRICA)?

The above has described the current articulation and implementation of information security policy by the post-apartheid South African state and explored some of their constitutional and legal weaknesses. It is arguably in the interests of the state as well as of civil society to address these weaknesses and place South African information security policy more

clearly on a constitutional foundation. The good government rationale of transparency should be given effect.[36] Furthermore, the broad confidentiality fostered by the Protection of Information Act and the MISS runs directly counter to the latest thinking of the last ten years or so regarding the effectiveness of a public sector in partnership with the private sector. The levels of confidentiality the NIA attempts to impose appear cumbersome and counterproductive.

Research in several areas would provide useful information regarding practical ways forward. Without being comprehensive, several may be mentioned here. First, with respect to the Appendix B declarations, one should attempt to get an indication of their use and effectiveness. Even though these declarations are governing policy, individuals may well refuse to sign these declarations on the above grounds of lack of authority and unconstitutionality. Second, with respect to the security clearance process and the NIA monitoring, one should monitor the extent to which the system is operative in government practice. One should also monitor the existence and operation of general policies of confidentiality in line with the AIA and specifically derivative of the AIA (as well as the imminent Privacy Act) rather than of the Protection of Information Act. It is possible that government policies of information security will be built on a department by department basis with a foundation of AIA principles. This would represent a decentralized approach rather than the older centralized policy.

Based on the research thus far, my view is that the Minimum Information Security Standards cabinet policy should be scraped. The replacement policy should be based upon the provisions of section 41 of the Promotion of Access to Information Act not on the Protection of Information Act. Likewise, the Protection of Information Act itself should be revised to fit within constitutional restraints while still providing for document handling procedures and the classification of national security information. There are some indications that revision of the MISS and of the Protection of Information Act may soon become priorities of the government.[37] The Minister of Intelligence Lindiwe Sisulu announced in Parliament in June 2002 that a review of the classification of documents should be instituted.[38] In March 2003, she announced the formation of a classification and declassification review committee. This committee has relatively strong civil society representation in its personnel. Furthermore, it is apparently mandated not only to review the criteria

and classification of apartheid-era information, but also to review the formulation of the MISS and the Protection of Information Act as well as the National Archives Act and the National Strategic Intelligence Act. It also appeared possible that amendments might be suggested to the Promotion of Access to Information Act. The announced intention was to review the MISS and elevate its status to that of regulations. This would be a significant step towards transparency and would afford civil society significant opportunities to influence the formulation of the revised MISS. This committee has asked for submissions by 30 April 2003 to guide its work.

THREE GLOBAL STORIES

To expand the focus beyond the narrowly national, it may be that South Africa's recent history of information security is at the confluence of three global stories of institutional development.[39] These three stories or trajectories undoubtedly overlap and interact in a variety of ways in different locales and political situations.

The first two of these stories can be traced back to origins in the U.S. One story is that of the diffusion of national rights to information laws. There has been a rapid diffusion of these laws since the late 1980s. The second story concerns the diffusion of secrecy laws, as Roberts shows in his paper.[40] Based on the model of American military secrecy, there were two bursts of diffusion of these laws, first in the development of NATO and second in the expansion of NATO into the countries of Eastern Europe following the end of the Cold War.

The third story of informational policy development is one that more global and may indeed be one where the South African story itself has played no small role. It is the story that Robert Horowitz tells in his analysis of the developments in the South African communications sector since 1994.41 In Horowitz's account (although the right to information does not figure prominently), civil society largely won and restructured the communications sector along a model of participatory citizenship. This third story of participatory and informed citizenship seems also to be the story that Deidre Curtin tells in her paper, albeit in the context of information communication technology in the European Union.[42]

It may be that this third story is one that is presently unfolding in Africa and with particular impact. Throughout Africa, ministries of information are facing serious challenges. National information security policies in countries such as Ethiopia and Nigeria are potentially in transition with ongoing legislative drafting efforts for right to information laws. The challenges to top-down government communications strategies come from other government organizations as well as from individuals and new communications technologies and media interests. The reception and impact of mobile phone networks may be one part of this broad trend. This trend may represent more than the adoption of specific laws and may be an expression of an emergent model of participatory and informed citizenship.

THE INFORMATION-SECRECY LINKAGE

It may be worthwhile to briefly note that the first two stories described above have some close linkages in practice and in law. The linkage mechanisms between the right to know laws and the secrecy laws may be as important to analyze as their respective substantive policies on national security information. In particular, through several legal mechanisms, these secrecy laws are often incorporated into the content of freedom of information laws. One mechanism is the classification of information by the military. This is the U.S. model. A second mechanism of incorporation is through the explicit presumption granted to another piece of legislation, a secrets law, whose content then in practice trumps that of the right to information law. This may be explicit in the law or through the operation of the later in time rule. This is the situation in Bulgaria and in other Eastern European states.[43] A third mechanism is through the protection of information rendered confidential through international agreements. The content of the international agreement is then imported into the domestic legal order. Even without these legal mechanisms, these secrecy laws may well be enforced through the bureaucratic power of the military. It may be that there are other legal mechanisms as well to link the substantive content of the secrecy rules to the right to information laws.

In South Africa, it is the third of the formal mechanisms that may potentially be used. Section 41(1)(b) of the AIA protects information that is required to be held in confidence by an international agreement. There

is an international agreement in force with the United States: the 1998 General Security of Military Information Agreement.[44] However, the operation of this mechanism in the South African context remains untested. Greater research needs to be done on the content and status of the international security agreements that the South African state has concluded with other states.

To date, the Protection of Information Act and the MISS itself have been the sources of the implementation or bureaucratic power exercised by the South Africa military and intelligence communities. The existence of this nationally-driven pressure for increased secrecy is an important feature that may distinguish the South Africa national security information policy dynamics from the countries of NATO implementing the Security of Information (SOI) policy of NATO, as Roberts shows. One may use the criteria of breadth, depth, centralization, controlled distribution and personnel controls - the criteria applied by Roberts - to analyze the MISS. In these terms, the MISS is one of breadth, centralization, controlled distribution, and personnel controls. The element of depth is however apparently a contested one as the operation of the review classification committee demonstrates.

Within this policy field, the focused interpretive and implementation power of the military/intelligence community certainly overshadows that of the set of government agencies given various responsibilities in the implementation of the Promotion of Access to Information Act: the Department of Justice, the Human Rights Commission, and the Government Communication and Information Service. There is no specialized enforcement body for the right of access to information, although advocates are pushing for such a mandate to be combined with a specialized body to enforce the privacy/data protection law currently early in the legislative drafting process.

Despite the organizational power of the South African military and intelligence bureaucracies, it does seem significant that their power has been at least partially exercised through legal forms. The preamble to the MISS is one example. That power has also been exercised under the shadow of a constitutional right of access to information backed by a judiciary with the power and will to enforce that right. It is remarkable that legislation restricting disclosure of information passed after the right to information law in South Africa has been careful to be consistent with the 2000 law.[45]

CONCLUSION

Elaine Scarry offers a piercing analysis of national security in the wake of September 11.[46] She argues for a citizen-focused version of national security. She points out that the only (apparently) successful defense of the four airplanes seized on that day was accomplished not by the F-15s deployed by the defense networks but rather by a group of the individuals aboard one of the airplanes. In her analysis of the event, a key feature is the rapid diffusion of information from and to the passengers on the airplane through the use of cellphones and on-board telephones. She concludes by arguing in favor of decentralized (citizenship-based) rather than centralized modes of national defense.[47]

This episode is relevant because it shows a direct relationship between a vision of citizenship and the concept of national security. Usually, the argument for greater information improving national security is made indirectly. In one indirect version, greater information accessibility entails greater accountability and thereby better national security. In another indirect version, greater information accessibility provides more and more accurate information to centralized military authorities who may then use that information to provide better national security. Elaine Scarry's analysis of the 11 September story shows the strong version of the argument in favor of a citizen's right to information. It shows at least one plausible episode where the benefit to national security is more than indirect.

A final observation comes with the relaxation of the assumption of a military based definition of national security. When one starts to think of national security in an expanded sense, one of the most important of those senses in the South African context is the achievement of socio-economic rights.[48] These rights are guaranteed in the South African Constitution and have been enforced and found justiciable in a series of cases by the Constitutional Court of South Africa. The role that the right of access to information may play in the promotion and protection of socio-economic rights is only beginning to be explored.[49] For the achievement of this understanding of national security, the right of access to information is crucial. Furthermore, it is likely that the practices and concepts developed within the military field of national security will influence practices throughout the field of national information policy.

NOTES

[1] The first several sections of this chapter draw on J. Klaaren "National Information Insecurity? Constitutional Issues Regarding Protection and Disclosure of Information by Public Officials" in (2002) 119 *South African Law Journal* 721-732.

[2] See generally, I. Currie and J. Klaaren *The Promotion of Access to Information Act Commentary* (SiberInk, 2002). Current developments regarding the AIA are available at the RULA website at www.law.wits.ac.za/rula.

[3] See I. Currie and J. Klaaren *The Promotion of Access to Information Act Commentary* (SiberInk, 2002) 173-177 for a more detailed examination of section 41.

[4] The Cameron Commission determined that South African policies regarding the provision of weapons to countries with poor human rights records should be made public. J. Klaaren and G. Penfold, "Access to Information" in M Chaskalson et al. (eds) *Constitutional Law of South Africa* (Juta, 2002) 62-21.

[5] In an important difference from the US Freedom of Information Act, the AIA does not reference or incorporate a classification system for the information security of records. Civil society resisted attempts to use the language of classification during the drafting of the legislation.

[6] The text quoted here is taken from s 4(1)(b)(iii) and (iv). Section 4(1)(b)(v) is even broader.

[7] Section 5 criminalizes providing aid to gain access to a prohibited place. Further sections of the Protection of Information Act regulate the onus of proof and other incidental matters. Other legislation targets specific sectors such as the defense Act 44 of 1957 and the Armaments Development and Production Act 57 of 1968.

[8] Para 5, MISS.

[9] Para 8, MISS.

[10] The preface notes how the MISS will be amended and such amendments distributed: "Any comments or recommendations in respect of this policy must please be forwarded in writing to the Chairperson of the Functional Security Committee of NICOC. All amendments to this policy will be issued by the National Intelligence Agency being the department national responsible for counter-intelligence. Government departments, institutions, parastatals and private companies will be responsible for the distribution of such amendments within their own organizations."

[11] Institution is defined to mean "any department of State, body or organization that is subject to the Public Service Act or any other law or any private undertaking that handles information classifiable by virtue of national interest." SANDFO/INT DIV/R/2/97 A-2.

[12] See Appendix A of the MISS.

[13] SANDF Order A-1.

[14] See for instance, para 3.1 and para. 4.

[15] For a historical examination of the military and the South African state, see A. Seegers, *The Military and the Making of Modern South Africa* (1996).

[16] MISS p. 8.

[17] Of course, one could argue that the South African (e.g. apartheid) tradition was precisely to define national security beyond military/security/intelligence matters.

[18] See MISS Preface and para 4.

[19] MISS paras 3 and 4, chapter 1.

[20] In other words, the definition of classified information in the MISS could (and one can argue to a court should) be interpreted only to cover information which must — in terms of some law or policy deriving from or consistent with the AIA — be exempted from disclosure. See further "National Information Insecurity?".

[21] One could make an AIA request for the number of employees in government with security clearances beyond the security services. From conversations with public officials, it appears that the information security measures are inconsistently applied even at senior levels.

[22] See Appendix A of the MISS.

[23] This form is provided in Appendix D of the MISS.

[24] The controversy regarding the questioning of members of the Presidential press corps on sexual partners and relationships indicates the extent to which questioning either by questionnaire or in an interview may go, although those questions were posed by the Secret Service, a separate security/intelligence service from the NIA. See V Harris "Sex, Spies, and Psychotherapy" available at http://www.wits.ac.za/saha/foi_reports.htm.

[25] See MISS, para 10.1, p. 50.

[26] The only reference to the declaration in the MISS is in responsibilities of heads of institutions where one responsibility is to "ensure that persons dealing with classified matters sign the prescribed declaration of secrecy (see Appendix B, a draft declaration that can be modified to suit the requirements in each particular case)[.]" MISS, para 10.5, p. 51.

[27] See "National Information Insecurity?".

[28] See *Dawood v Minister of Home Affairs* 2000 (3) SA 936 (CC) (state may not depend upon the limitation clause where a fundamental right is implicated and no guidelines are provided).

[29] 1996 (4) SA 965 (NmS). This discussion is taken from Marcus and Spitz, below.

[30] Thereby violating either the principle of legality or the right to just administrative action or both. Still, the charge of overbreadth does not automatically lead to unconstitutionality. *Poswa v MEC for Economic Affairs Environment and Tourism, Eastern Cape* 2001 (3) SA 582 (SCA) (in anti-corruption context).

[31] The evaluation of unconstitutionality is supported by G. Marcus and D. Spitz in "Expression" ch 20 in M Chaskalson et al. (eds) *Constitutional Law of South Africa* (revision service 3, 1998) at 20-28.

[32] Other ongoing conflicts over access to information are also directly relevant to the issue of national security. In particular, the South African History Archive (SAHA) hosted a 2002 conference aimed at exploring ongoing South African government secrecy with respect to the history of South Africa's nuclear weapons and development program. See *http://www.wits.ac.za/saha/nuclearhistory/index.htm*. Furthermore, SAHA has successfully applied for access to the so-called "sensitive documents", the 8/2 files used by the National Archives for sensitive materials during the 1960s and the 1970s. See http://www.wits.ac.za/saha.

[33] This section draws on V Harris "Telling Truths About the TRC Archive" available at *http://www.wits.ac.za/saha/foi_reports.htm*.

[34] While the CCII case is one that implements the AIA, earlier South African cases had implemented the constitutional right of access to information directly. This is a contrast from the situation in Bulgaria. See A. Kashumov's contribution to this volume, "National Security and the Right to Information in Bulgaria," at 4.

[35] For more background and a legal analysis of this case, see "Analysis of the Judgment in CCII Systems (Pty) Ltd v Fakie NO (January 2003) available at http://www.wits.ac.za/saha/foi_reports.htm.

[36] See in the 1996 Constitution, the principle expressed to guide the public administration in section 195(1)(g): "Transparency must be fostered by providing the public with timely, accessible, and accurate information."

[37] This paragraph draws from stories in the Sunday Independent (8 March 2003), the Sunday Times (8 March 2003), and SABC Online (8 March 2003).

[38] Business Day (6 June 2002) "Apartheid era documents might soon be declassified."

[39] Here, I am using the notion of stories of development that Alasdair Roberts has employed in a recent paper. "These Patterns in the Diffusion of Transparency Rules: Money, Guns and Human Rights," presented at the Workshop on the Internationalization of Regulatory Reforms, University of California (Berkeley), 25-26 April 2003. However, my specification of the three stories differs slightly. As explained in the text, for the third story, I see a more global and expanded story of citizenship development within the communications sector rather than a particular move towards greater informational accountability on the part of international financial institutions.

[40] A. Roberts ,"NATO's Security of Information Policy and the Right to Information".

[41] Robert B. Horowitz, *Communication and Democratic Reform in South Africa* (Oxford University Press, 2001).

[42] See D. Curtin contribution to this volume, "Digital Government in the European Union: Freedom of Information Trumped by "Internal Security" (see particularly at 13-14).

[43] See A. Kashumov, "National Security and the Right to Information in Bulgaria".

[44] Communication from A Roberts (28 April 2003). Obtaining this 1998 Agreement, one could then compare the South African agreement to the breadth, depth, centralization, controlled distribution, and personnel controls of the apparent shape of the NATO policies as well as examine the effect or lack thereof of the agreement on South African informational security law, policy, and practice.

[45] One example is the Financial Intelligence Centre Act.

[46] E Scarry "Citizenship in Emergency: Can Democracy Protect Us Against Terrorism?" *Boston Review* (available at http://bostonreview.mit.edu/BR27.5/scarry.html).

[47] Tom Blanton's contribution to this volume also alludes to this citizen defense example. See Blanton at 29-34. In this sense, I would agree with Blanton that one needs to go beyond the balance metaphor. The challenge would be to develop an information regime that both directly incorporates national security and directly incorporates the informational dimension of citizenship.

[48] It is of course possible to contest the definition of the concept "national security". One way might be to distinguish between military security, political security, and bureaucratic security. Another way is to use the term security for other policies and programmes than military ones. For instance, one can speak of food security. To this point, this paper has used a military definition of national security.

[49] See J Klaaren "A Second Look at the Human Rights Commission and the Promotion of Socio-Economic Rights" (paper delivered at the South Africa Reading Group of New York Law School and the Constitutional Roundtable of the University of Toronto Faculty of Law) and R Calland and A Tilley (eds) *The Right to Know, the Right to Live* (2002). A recent case uses the constitutional right to information but not the AIA to order the government to hand over some documents related to the arms deal. See "Govt given 10 days to hand over arms documents" *Mail and Guardian* (27 March 2003).

NATIONAL SECURITY AND OPEN GOVERNMENT IN INDONESIA

Bimo Nugroho
Director, Institut Studi Arus Informasi Indonesia

I should ashamedly admit that my country, Indonesia, has the most corrupt bureaucracy. Without quoting any data by credible international institutes, I dare to make this confession because I have experienced myself how difficult and costly it is to get a passport, to process birth certificates for my children, and even to have an ID card stating that I am a citizen of Jakarta, the capital of Indonesia.

Citizens have access to general information about the procedures they need to follow to obtain a passport or ID card and about the standard costs they would incur, but in practice, the procedure leads them into a frustrating labyrinth. The process either is very time-consuming or yields no results, because the public officers who are responsible do their jobs only half-heartedly. Eventually, Indonesian citizens – frustrated and facing time constraints – usually choose to spend some additional money to bribe the public officers for a passport or ID card.

Indonesian citizens have watched this happen helplessly for a long time. Public officers are the government's instruments, who have their roots in the authoritarian and repressive Suharto regime. The Suharto regime has ruled Indonesia for 32 years. Protest is a luxury the citizens cannot afford. Those who have the courage to protest must be prepared to be socially sanctioned, labeled as communist, or jailed.

Fortunately, however, Indonesian youth, students, and intellectuals never stop protesting. They all are like drops of water that devotedly fall into a

stone and, as a result, break the stone. In 1998, Suharto resigned as President unable to resist the continuous wave of student rallies that rode on the acute economic crisis that battered the entire Southeast Asian region.

However, corruption in Indonesia is more stubborn than Suharto. Public officers and the citizens have grown accustomed to the state's closed government and lack of civil control. It is the nation's deepest wish to eliminate corruption. Hundreds of non-governmental organizations (NGOs) nationwide have been contributing their expertise in their respective sectors. My organization, the Institut Studi Arus Informasi (ISAI), is only a small component of the efforts to promote freedom of press and freedom of information, which would allow corrupt practices to be uncovered. There are many other active organizations, such as the Indonesian Corruption Watch (ICW), which focuses its activities on unraveling corrupt practices, and the Indonesian Center for Environmental Law (ICEL), which fights against the robbery of Indonesia's vast natural resources through regulations that promote transparency.

The ICW, ICEL, ISAI, and many other non-governmental organizations are forming the new Coalition for the Freedom of Information. The coalition aims to draft the Freedom of Information Bill, perform intensive lobbies of the House of Representatives (DPR), undertake campaigns through mass media and other public forums, and mobilize the people at the grassroots level to demand their right to information that public officers should provide.

The people of Indonesia believe the country's authoritarian government encourages corruption, collusion, and nepotism — known by the acronym "KKN" — and human rights abuses. All of these practices are institutionalized and internalized, because the people cannot control the state or its public officers. As a result, the public officers do their jobs half-heartedly and arbitrarily. They feel no need to provide the public with information and accountability reports because no rule requires them to do so.

Indonesia needs a Freedom of Information Act. The House of Representatives has been deliberating how to achieve this, but it is a long and winding road. During deliberations, there have been severe battles between the Freedom of Information bill and the State Secret, Antiterrorism, Intelligence, and Indonesian Armed Forces bills. The

September 11 terrorist attacks in the United States and the Bali blast prompted these discussions. Former Suharto loyalists and the military forces that previously supported the smiling general's leadership now have another chance to perpetuate the closed system of government in the name of national security. Now, Indonesian people face a confusing dilemma: should they choose an open government at the risk of uncontrolled freedom or a closed government that can maintain the stability required for an economic recovery?

The alternatives are more complicated by the fact that Indonesia is a poor country. We will be at greater risk if we fail, and we have little time to reflect and choose. This complexity makes the problems in Indonesia more interesting and challenging to solve.

This paper systematically :

(1) describes Indonesia's deeply rooted closed regime;

(2) explains efforts to promote transparency through civil movements to realize the Freedom of Information Act;

(3) discloses the anti-change responses communicated through the State Secret, Antiterrorism, Intelligence, and Indonesian Armed Forces bills; and

(4) presents options that are feasible within a tight timeline, as the general election of April 5, 2004 approaches.

Deep in my heart, I hope our discussion in this forum will not only serve as an academic one. Rather, it should be able to provide realistic inputs for the world, especially Indonesia, in changing the existing order. I come here from a far country, and I have had to fight for a visa to get here due to the Iraq war. Therefore, it is only natural for me to expect all of you to pay more close attention on Indonesia. After the general election on April 5, 2004, we may start from "square one."

INDONESIA'S CLOSED REGIME

The transitional era in Indonesia inherited the closed and secrecy-based system and culture of the Suharto regime. Steven Aftergood distinguish-

es between the genuine national security secrecy, political secrecy, and bureaucratic secrecy.[1] In Indonesia, political secrecy and bureaucratic secrecy are the most common.

Big ruling parties and the government's bureaucrats classify information as secrets without any clear standards or procedures. Secrecy classification has become a mechanism to conceal the public officers' lies from the public eyes. It is created to hide "KKN" practices, human rights abuses, and military violence against civilians that will tarnish the image of public officers. When Suharto was in power, military secrecy, bureaucratic secrecy, and national secrecy often were used to prevent the public from accessing information that state institutions controlled. Now, three presidents have succeeded Suharto — Habibie, Abdurahman Wahid, and Megawati — but the secrecy classification continues, in accordance with the state apparatus' interests and with the level of public demand for transparency. If public pressure is strong, a state officer often will provide the requested information out of fear of being ousted by his or her political opponents.

There are many cases of excessive secrecy. Some are considered military secrets and some are classified as bureaucratic secrets. Below are the still unresolved secret military cases:

- The role of Suharto's political machine in the mass murder of Indonesian Communist Party (PKI) followers between 1966 and 1970. Many analyses have been circulating about this, including a theory that the CIA might have been involved by supporting Suharto in the murder of PKI followers, or that Suharto himself did the murder, relying on military support;
- The military's role in imprisoning and killing Muslim fundamentalist activists; and
- Policies in Indonesian military operational regions in East Timor (now an independent country) and Aceh. The number of the dead victims is unknown and it is not clear who should be held responsible for the killings in the regions.

Mass murder cases are difficult to solve because of their structural and cultural complexity. Thus far, there is no regulation that protects witnesses' safety. Eyewitnesses to the murders, most of whom have grown old, are afraid of what military personnel would do to them if they

spoke up. Although the political power of the armed and police forces has been declining, their personnel still have strong economic bases, built while they were still in power. Businessmen (in national and multinational firms) who need security services in their business area are other profitable machines.

It will take a long time to eliminate the Indonesian people's fear of military and police forces. It is this fear that has saved the military officers from being held accountable for mass murder. They even avoid being held responsible for the killings of communists, because the country's rulers have indoctrinated society to fear communism and communists. Furthermore, the military officers also get away easily from their sins of mass killings in East Timor by hiding behind narrow-minded nationalist and patriotic sentiments that have been propagated by some rich generals in public fora and the mass media.

Aside from the military cases, during the transitional era many secret cases involving bureaucrats and public officers have been revealed. Some examples of the notorious cases that have been tried in the Indonesian court include the Akbar Tanjung case and the case of Central Bank:

> Akbar Tanjung currently is the Speaker of the House of Representatives (DPR) and also Chairman of the Functionaries Group (known as the Golkar party), the second-biggest Indonesian party after the struggling Indonesian Democratic Party (Partai Demokrasi Indonesia, or PDI-P), led by President Megawati Sukarnoputri. In 1999, while serving as state secretary in President Habibie's cabinet, Tanjung secretly allocated the funds that belonged to the Yanatera Foundation of the State Logistics Agency (Bulog) to Golkar to finance the party's election campaign. Two levels of courts (district and appeals courts) have found Tanjung guilty, which would have been impossible in the Suharto era. Now, the case is being processed in the Supreme Court for a final verdict.

In democratic countries, public officers like Tanjung should resign from their political positions in both the parliament and the political party. However, in this transitional era when the power tensions are high, the embattled Tanjung stubbornly stays in his position to lead the Golkar

party, fighting to win the general election of 2004. He also retains his position as the Speaker of the House of Representatives and, along with Golkar functionaries who support Tanjung's stance, annuls every session with an agenda to oust Tanjung from his position. All evidence has been made public, but Tanjung's lawyers cleverly hide behind the "presumption of innocence" principle, which they say should be applied until there is a final decision from the Supreme Court. Besides, there is no regulation that requires the Speaker of the House of Representatives to resign, even though there are already guilty verdicts in the district court and appeals court.

> In another case, the directors of the Central Bank (BI) have been found guilty and jailed for secretly allocating funds from a Central Bank loan to ailing private banks that were battered by the 1996 economic crisis in Asia.

Before the transitional era, collusion between public officers and businessmen was a common practice. Today, collusion still remains and grows in complexity. Therefore, it is becoming more crucial to fight for clean, open, and good government.

THE CIVIL MOVEMENT TO CREATE OPEN GOVERNMENT

One major cause of rampant "KKN" and human rights abuses in Indonesia is a lack of societal control over the state. Therefore, one principal remedy would be to empower the civil society's position vis-à-vis the state, so that the civil society could access information about bureaucratic processes and the management of public resources.

At this point, there emerges a need for a regulation that ensures the institutionalization of transparency, informational openness, and public participation principles. It is urgent to have an act that guarantees and regulates the public's rights to obtain information about the government and that requires the public institutions to provide such information. The Freedom of Information Act would fulfill these needs.

However, it is impossible to rely solely on the government's good will

to realize the Act. This is why in December 2000, several non-governmental organizations fused themselves into a civil society coalition called the Coalition for the Freedom of Information. The coalition aims to garner support from pro-democracy elements to fight for adoption of the Freedom of Information bill.

At the present time, the Coalition for the Freedom of Information consists of 40 non-governmental organizations and various professional associations. The coalition has drafted and implemented several working agendas since it was formed. Ultimately, the House of Representatives adopted the Freedom of Information Bill as an initiative bill during its plenary meeting of March 20, 2002. Almost a year later — on February 18, 2003 — the Special Committee of the House of Representatives was established to begin deliberating on the Freedom of Information Bill, article by article. The Coalition for the Freedom of Information has been trying to encourage the Special Committee's work through lobbying, drafting articles, a media campaign, and public pressure.

In general, the civil movement to promote the freedom of information has begun to influence public opinion. The mass media has begun to adopt the "freedom of information" perspective more intensely to spotlight violations in the government. A freedom of information discourse has also developed at the regional level. Local partners of non-governmental organizations and universities have held several discussions to talk about the performance of public institutions that have maintained secrecy and been stained by "KKN." They have also begun to emphasize the importance of drafting transparency laws at the regional and local level.

President Megawati has also issued a political statement conducive for the next political process to deliberate the Freedom of Information Bill, although the statement has yet to be followed up. However, the bureaucracy has shown strong resistance to the open government idea.

RESPONSE IN THE NAME OF NATIONAL SECURITY

Resistance to openness got new momentum after the Bali blast on October 12, 2002. After this incident, President Megawati signed the

Anti-Terrorism Regulation proposed by the National Intelligence Agency (BIN) without any hesitation. Spurred by the September 11, 2001 attacks on the World Trade Center, the National Intelligence Agency — which is still dominated by former President Suharto's military loyalists — proposed a draft policy which permits the intelligence apparatus to detain any suspicious people who may harm the national security, without legal procedure. The Agency's policy has received strong criticism from intellectuals who argue that in the past, ruling presidents have often abused such rules to paralyze their political opponents.

Meanwhile, the military faction that still wants to be fully engaged in the political world is not satisfied with the anti-terrorism act alone. The House of Representatives has also passed the State Secrets bill proposed by the State Code Agency. This step was not necessary, as the Freedom of Information bill already contains articles on special information the disclosure of which might threaten the national interest. In addition, Indonesian Armed Forces (TNI) have proposed the Indonesian Armed Forces bill, which has sparked media criticism because of its provision that the TNI can act within 24 hours to protect the national security without the president's permission.

AT THE CROSSROADS

If I could choose between government openness and national security as Indonesia's top priority, I certainly would favor government openness. My reasoning is simple: in a transitional country such as Indonesia, real national security would be achieved by creating an open government. The openness that the Freedom of Information Act would guarantee would expand bureaucrats' responsibilities and promote public participation to protect the national security even on the smallest scale.

On the contrary, "national security" enforced with a militaristic approach would only create false security – security fostered by the fear and hatred of military victims. Police investigations of the bombings in Jakarta and Bali have provoked strong suspicions that the attacks were performed by hardline activists that hid behind Islam — the products of decades-long political repression of Islam by the government.

Repression through militaristic murders has triggered hatred that is ready to explode any time. Militaristic solutions for national security have proven ineffective. Civilians became victims in East Timor and Aceh, and now the former is an independent country and Aceh is still choked by rebellions.

For the civil society in Indonesia — especially the critical elements such as students, NGOs, and intellectuals — the best choice is to create a legal guarantee through the Freedom of Information Act, founded on the principle of government openness. With this law, Indonesian civil society will have a sound legal basis to get public information, access information freely, and ask public officers to account for cases that affect the public interest.

It is this choice that is being actively promoted within the remaining short time until April 5, 2004, the date of the general election that will elect new representatives for to Parliament. Many Indonesians' deepest hope is that their new representatives will be better. But, if money politics has a hand in it, the election will produce only self-centered and bad representatives. In poor countries like Indonesia, only the corruptors have what it takes – in this case, money – to win seats in Parliament. If that happens, the struggle for an open government will revert to ground zero.

NOTES

[1] Steven Aftergood, "Secrecy is back in fashion," *Bulletin of the Atomic Scientists*, 56.6 (November-December 2000), pages 24-30. http://www.thebulletin.org/issues/2000/nd00/nd00aftergood.html.