Translucence Not Transparency

ELIZABETH RINDSKOPF PARKER*

Reviewing ALASDAIR ROBERTS,
BLACKED OUT: GOVERNMENT SECRECY IN THE INFORMATION AGE
(CAMBRIDGE UNIVERSITY PRESS, 2005).

ABSTRACT

All doubts about the importance of reconsidering government secrecy, openness and accountability as the post-Cold War world confronts the Information Age are rapidly dispelled by Alasdair Roberts' Blacked Out: Government Secrecy in the Information Age. Professor Roberts explores the evolving tension between traditional diplomatic secrecy and the increasing open nature of modern democratic governments. In the post-Cold War world, information sharing networks extend far beyond the bilateral information sharing networks that pre-dominated the Cold War world. Such arrangements often present difficulties in knowing just who provided the original information—a problem that accounts for a growing lack of transparency where networks are obligated to honor the control requirements of the originating nation. Ironically, there is transparency within the network, but opacity to those outside the standard is no longer transparence but translucence. Equally troublesome is the increasing amounts of information being withheld from public disclosure under a "sensitive but unclassified" rubric. The author argues that information access systems have become confused as the boundary between private and public activities, particularly with regard to national security, have been obscured. In conclusion, the author discusses the growth of data in electronic form and finds that such aggregate data carries with it a threat to personal privacy as well when private organizations use such capabilities to assemble extensive knowledge about individuals from widely distributed public records. It is a book important for anyone concerned with the history and future challenges of government information access at a time of fundamental change.

All doubts about the importance of reconsidering government secrecy, openness and accountability as the post-Cold War world confronts the Information Age are rapidly dispelled by Alasdair Roberts' Blacked Out: Government Secrecy in the Information Age. Not everyone will agree with all of its conclusions, but no one can

---

* Dean, University of the Pacific, McGeorge School of Law.

question the value of this tour de force. It is a book important for anyone concerned with the history and future challenges of government information access at a time of fundamental change.

Beginning with a review of the origins of government policies controlling access to information, Professor Roberts explores the evolving tension between traditional diplomatic secrecy and the increasingly open nature of modern democratic governments—a theme he uses to organize much of the discussion of this valuable contribution. This doctrinal change, from presumed secrecy in government matters to the people's right to know, has fundamentally altered the nature of government. For an increasing number of nations, the traditions of absolute governance which supported absolute privacy and secrecy among rulers have now largely vanished. A surprising number of countries, following the U.S.'s lead, have enacted their own[1] legislation providing citizens the right to access government information.

Nevertheless, these nations do not reflect an even and consistent application of the laws supporting governmental openness and accountability. Enforcement is typically a problem for those nations that could be described as "emerging democracies," constituting the second wave of adopters of openness laws. These nations are less affluent and not as politically stable as those that preceded them. Too often, government corruption is a serious problem for them. In response, perhaps not surprisingly, many such nations have created significant exceptions in their laws for state security. Certainly all of them struggle with enforcement of their access laws, a process which is both costly and heavily dependent upon sophisticated governmental bureaucratic machinery (including record-keeping, well-trained bureaucrats, effective court procedures and the availability of lawyers).

In fact, the adoption of these legal systems each reflects the special history of the several nations involved. As Professor Roberts concludes, nations have adopted access laws for a variety of reasons. Considering the U.S. experience, he connects the advent of government information access to the conservative response to New Deal reforms as well as concerns about the increase in information obtained and controlled by the newly created independent agencies.

---

[1] Professor Roberts reports that by the end of 2004, fifty-nine countries had adopted their own Freedom of Information Act. Among those mentioned prominently are Western powers such as Australia, Canada, New Zealand, the United Kingdom, France, German laender (although not the federal government), Sweden, Finland, Denmark and Japan. More surprising, however, are the recent adopters in emerging democracies such as Mexico, Pakistan, Guangzhou, China, Kenya, Jamaica, Uzbekistan, Nigeria, Uganda, South Africa, and India.

The 1946 Administrative Procedure Act, responding to this situation, provided the ground work for the later 1966 Freedom of Information Act (FOIA). Ironically, the interest in such government accountability through access to information shifted across the political spectrum with Ralph Nader and environmental interests championing the new FOIA law in the mid 1960's. Once in place, other Western governments eventually followed the U.S. model, adopting their own legislation. Ironically, U.S. leadership also demanded and obtained restrictive information protection policies for its NATO allies in the 1950's.

In other cases, traumatic national experience provided the basis for adopting freedom of information laws. Here the experience of Argentina, Brazil, Chile, Peru, Paraguay and South Africa share common origins. Even so, for some the curative power of such new access to information laws has been limited by exceptions included in the provisions of these laws, particularly with regard to information involving intelligence and the military—the sources of prior governmental abuses. In other cases, local courts have ruled in ways that carve out portions of the bureaucracy most in need of openness provided by information access laws.[2]

In the end, while an anomaly measured against international standards when originally enacted by the United States,[3] freedom of information laws are now considered an international standard expected of all nations desirous of entering the world economy.[4] Moreover, adopting such openness policies is now seen as a pre-condition to creating a successful democracy. Even so, Professor Roberts concludes that access laws may correlate with or support good governance, but do not necessarily cause it.

This trend toward greater openness is not without its modern-day challenges. Professor Roberts describes a variety of "head winds," beginning with the Bush Administration's response to current world

---

[2] For example, both Latvia and Slovakia have had court decisions holding that there is no "human right to classified information," while India's law excludes all nineteen of its intelligence collection agencies.

[3] Sweden and Finland appear to have been earlier adopters of their own access laws.

[4] U.S. legislation in support of governmental openness includes a broad range of legislative provisions including: the Presidential Records Act (1974), the Privacy Act (1974), the Ethics in Government Act (1978), the Government Sunshine Act (1972), the Federal Advisory Committee Act (1972), the Civil Service Reform Act (1978), the Inspector General Act (1978), the General Accounting Office Act of 1980, and the Foreign Intelligence Security Act (1998).

threats from terrorism, as well as decisions in Australia, New Zealand and Canada to permit the blacking-out of information in response to governmental claims for secrecy. In short, powerful tensions between secrecy and security have been revealed in response to the "War on Terrorism." And, as responses to this threat have matured, Professor Roberts sees increasing reliance on secrecy to protect government information that might be used to harm national security. For example, al Qaeda's caves at Tora Bora revealed an extensive study of maps of critical U.S. infrastructure, justifying further restrictions on the wide-spread release of such information on the internet. This new category of information, "critical infrastructure information," has become the subject of increasing attention and is the justification for the growth in another category, known as "sensitive but unclassified" restricted information. There has also been far too little funding support for effective implementation of access legislation in the U.S. and elsewhere. Declassification efforts are under-funded and so, too, are efforts required to respond to FOIA requests.

At a fundamental level, of course, the real problem now is how to judge the value of secret information--does it support, or undercut, our security? Here Professor Roberts makes an important point: The fact is that in the post-Cold War world, we risk over-protecting what is important to our security. How can citizens respond effectively to national security threats if they do not understand them? A second issue may be that, without transparency into government decisions, wise choices about our security would be impossible to make. How then do secrecy and security relate in the post-Cold War area?

In Roberts' view, "[n]ational security was compromised by the secrecy that surrounded war planning exercises and efforts to improve homeland security." I could not agree more. We need a far better understanding of the world in which we live. The government's failure to share information more readily before and after 9/11 limited our understanding, our ability to imagine the worst, and to prepare adequate responses.

Meanwhile, the information age is changing how governments function, which in turn causes a rethinking of how we manage open government. First, like many governmental officials, the current Bush Administration has found governing in the conditions of openness that currently exist increasingly difficult. The modern information age makes managing information far more difficult today than in the past. Certainly the level of information available makes controlling the agenda of any Administration problematic. Second, there is also the problem of "data overload." In some common law countries the response has been to seek mechanisms for central control of information requests, or to tighten what information can be released,

often by imposing fees. Unfortunately, in Professor Roberts' view, such efforts to control the release of information across the common law world have tended to backfire, further exacerbating the underlying crisis of government legitimacy.

Turning to the new intergovernmental structures which have developed in the aftermath of the Cold War, Professor Roberts' analysis challenges us to consider whether such structures have eroded traditional openness. He describes the problems of achieving intergovernmental collaboration when nations exist in differing states of sophistication with regard to information control and access. In the post-Cold War world, three information sharing networks among the nations of the world are emerging: defense, national intelligence agencies, and national police forces. This is the "new intelligence order," which is both deeper and larger, based on a much broader network of bilateral relationships.[5] These relationships extend far beyond the bilateral information sharing networks that pre-dominated the Cold War world. Such arrangements often present difficulties in knowing just who provided the original information—a problem that accounts for a growing lack of transparency where networks are obligated to honor the control requirements of the originating nation. The result for information access purposes is often a "lowest common denominator" solution in which the nation least willing to allow information to be released controls access decisions for all others. Ironically, there is transparency within the network, but opacity to those outside the standard is no longer transparence but translucence.

Following 9/11, this development has intensified. In Professor Roberts' view, the amount of classified law enforcement information has increased while the willingness to share it with the public has diminished. Here I must dissent. I believe the problem may not be as great as suggested. The relationship between federal and local law enforcement authorities is an asymmetric one. The information shared by federal authorities with local law enforcement has increased, but not the reverse. The information is classified and local authorities must protect it; but the public's access to it, or lack thereof, remains the same.

On the other hand, there can be no dispute that Professor Roberts is correct in asserting that too much information remains classified today. Increasing amounts of information are being withheld from public disclosure under a "sensitive but unclassified" rubric. An awareness of the vulnerability of critical infrastructures and related systems, the

[5] By way of example, forty-eight Mutual Legal Assistance Treaties are now in existence, and forty-three nations have joined the U.N. Convention on Drug Trafficking.

vast majority of which are controlled by the private sector, underpins much of this conceptual framework which has been designed in an ad hoc process to prevent its release. To be sure, more needs to be done to structure the way in which critical infrastructure information is managed. But, the fact that this information relates to potential vulnerabilities of interest to our terrorist foes is unarguable. There is certainly logic to efforts made to protect this information, even if they are clumsy or strain current legal authorities.

Nonetheless, Professor Roberts is correct in arguing that information access systems have become confused as the boundary between private and public activities, particularly with regard to national security, have been obscured. Added to this is the growing practice of "contracting out" government services as a money-saving response to the costs of doing business. It remains to be determined how information access will be managed for such contracted activities. Are they essential governmental services, subject to government information access, or private matters, free from public scrutiny?

In sum, what should the rights to information be when formerly government functions move to the private sector through the process of outsourcing? Professor Roberts does not answer this question, but provides useful analysis of considerations which will be relevant. One answer may be that access must turn on whether information is required to preserve traditional rights associated with citizenship. This choice is not one that is yet embodied in U.S. law where access to information has yet to be accorded constitutional status. Nonetheless, at least one nation, South Africa, has taken this step, providing the right to either public or private information in its Public Accountability Information Act (211) as long as a need has been established. How different is this than the U.S. approach where, little by little, access to information has been provided in individual pieces of legislation? Professor Roberts gives examples here as disparate as securities legislation or students' rights to campus security information. Equally important, but not mentioned, are the unique discovery features of the U.S. legal system where private litigants have the right to access private information relevant to proving asserted rights.

Turning to the growth of "supranational" institutions, Professor Roberts makes a valuable contribution in examining the reluctance of these organizations to adopt the full panoply of access to information rights of their various member nations. With the notable exception of the European Union, where access rights have been repeatedly upheld by the European Court of Human Rights, such organizations have reflected their diplomatic origins with a penchant for secrecy. The World Trade Organization, the World Bank and its subsidiaries, are all examples of organizations displaying extreme reluctance where

freedom of information is concerned. This is a story that Professor Roberts tells in convincing detail, documenting carefully both the resistance and the gradual adoption of greater accountability through openness.

As a final topic, Professor Roberts discusses the nature of the growth of data in electronic form. This explosion has been accompanied by new challenges of data management until the advent of metadata and capabilities such as Electronic Document and Records Managements Systems (EDRMS) which enable sorting and assessing the content of vast data sets. Disturbingly, such aggregate data carries with it a threat to personal privacy as well when private organizations use such capabilities to assemble extensive knowledge about individuals from widely distributed public records. Perhaps it will come as no surprise that the Freedom of Information Act, designed to allow the citizen to access records of the government, has, in the end, been turned "on its head." Now the ability to aggregate small bits of government-maintained personal information into comprehensive individual files threatens the individual's privacy. And, when such private compilations of data are sold back to the government, the very laws designed to protect the citizen have, at last, been turned against the citizen.

As Blacked Out: Government Secrecy in the Information Age shows, the Information Age is a time of unexpected and unintended consequences when many fundamental assumptions and values seem almost to turn on themselves. Above all, this is a time when Professor Roberts' thoughtful book is most welcome to those who study, manage or simply care deeply about the value of a means of achieving open government.