Transparency in jeopardy

Blacked Out: Government Secrecy in the Information Age

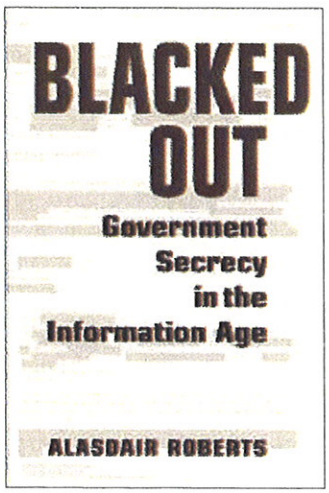
by Alasdair Roberts. New York: Cambridge University Press, 334 pp., 2006.

Peter P. Swire

Alasdair Roberts provides an excellent sense of the history and key issues of efforts to hold governments accountable by requiring the disclosure of information they possess. Roberts has a comprehensive knowledge of global trends, which he describes and analyzes eloquently. He is not as successful, however, at providing a workable theory for when transparency is appropriate in the face of the competing demands for homeland and national security.

Roberts, an associate professor in the Maxwell School of Citizenship and Public Affairs and director of the Campbell Public Affairs Institute at Syracuse University, begins the book, which is essentially a series of essays, by examining the heroic cause of revealing government secrets. He opens by describing the German Parliament in Berlin, built in the wake of the reunification of East and West Germany, where a milestone in transparency took place with the release of millions of dossiers held by the Stazi, the East German secret police. Topped with a grand cupola made of glass, the building serves as a metaphor for the book, or at least for its optimistic agenda of increasing transparency in government.

Roberts offers a paean to transparency on the march. The United States passed the Freedom of Information Act (FOIA) in 1966. Twenty years later, only 11 countries—other wealthy democracies—had promulgated similar statutes. By the end of 2004, however, 59 countries had adopted right-to-information laws. What prompted this change? Roberts says many of the former Communist countries of Eastern Europe followed the German pattern and opened secret files as part of the shift to democracy. Public interest groups, of which Transparency International is perhaps the best known, pushed for transparency statutes as a check against corruption and other wrongdoing. International institutions, including the World Bank, encouraged aid recipients to pass transparency statutes, and many Third World countries have recently passed FOIA-type laws for the first time.



Roberts shares a number of examples—taken from far-flung locations such as India, Thailand, Japan, Uganda, Mexico, and Great Britain (which only recently began to implement its first FOIA)—in which transparency has served as a crucial tool for improving government activities. The examples show how transparency has helped address problems such as corruption in public works, favoritism in school admission, tainted blood supplies, and all manner of other excesses of governmental efforts to control information and thus their populations.

Paralleling this optimistic story of increasing transparency, however, is a counter-narrative of increasing secrecy. The 9/11 attacks have given new vigor to the perspective that secrecy is required to protect national security. The Bush administration's push for greater secrecy began even before 9/11, most notably with Vice President Cheney's insistence that his energy task force not be subject to openness requirements. The Watergate-era reforms that are viewed so positively by supporters of transparency are seen by Cheney and other officials as lamentable incursions into the powers of the presidency.

Roberts catalogs the many shifts toward secrecy during the Bush administration, including more restrictive FOIA policies, new classification and declassification rules, widespread use of the "sensitive but not classified" designation, the dismantling of government Web sites, and refusal to answer press and congressional queries. Somewhat surprisingly and somewhat persuasively, he concludes that the administration's secrecy policies have not been entirely successful. He argues that whereas the transparency revolution that began with Watergate has become entrenched in statute, the Bush counterrevolution has not. I am not as sanguine as Roberts on this point. Because there have been so many recent secrecy efforts and because the government is still in the midst of defining the rules for the "long war" against terrorism, there are serious reasons to doubt that the current secrecy initiative has run its course.

Roberts goes on to explain the three trends he sees as threatening the march toward greater transparency, and here he is perhaps most compelling. The first trend is the development of what he calls "opaque networks." Although the 9/11 Commission and the 2004

reform of the U.S. intelligence system made information-sharing a major priority in the fight against terrorism, much less appreciated has been the way in which information-sharing undermines the efforts to promote open government. Robert writes: "Transparency within the network is matched by opacity without." For instance, cities and states that work with the federal government on homeland security face strict new limits on what they can disclose under their own FOI laws. At the international level, Roberts reports that many of the new democracies of Eastern Europe specifically passed national security and other limits on transparency at the insistence of the United States. To participate in new information-sharing networks, these countries had to promise not to disclose any secrets exchanged, even if their own antisecrecy laws said otherwise.

The second theme, called "the corporate veil," highlights how privatization reduces transparency. In recent decades, an unusual political coalition supporting transparency developed: Public interest groups that favored government accountability teamed with companies that favored limits on government power. More recently, however, the government has increasingly outsourced work to the private sector. Companies have then resisted requests to disclose information related to the contracts, arguing that disclosure would jeopardize competitive secrets. Transparency advocates, meanwhile, fear that this increased secrecy in government contracts will lead to unaccountability, so that work will be performed less well, at higher cost, and possibly corruptly.

Roberts provides a number of examples of this trend. One is the outsourcing of prisons, in which corporate managers resist disclosing embarrassing details such as the number of escapes or the level of medical care. Another involves companies that develop commercial databases and sell their products to government agencies. In the United States, with certain exceptions, the Privacy Act assures citizens the right to access their own files when the data is held in a government "system of records." But the act usually does not apply when the government obtains the same information about citizens from a private database company. These examples underscore the need to broaden the debate about when the government should outsource.

The third theme, on "remote control," highlights the role of supranational institutions. Transparency statutes have been promulgated largely at the national or subnational level. Government power, however, is shifting to supranational institutions such as the European Union, the World Trade Organization, and the International Monetary Fund, which largely lack transparency statutes. Roberts concludes that promoting transparency within such organizations will be an uphill battle, with success depending on political factors in each setting.

Critique falls short

Although Roberts provides a rich sense of how transparency regimes operate in different countries, he is less successful in providing a normative theory for deciding when more transparency is appropriate. There is no empirical evidence presented to show where there are net benefits of transparency. There is no philosophically rigorous attempt to define categories where transparency should be favored or disfavored. There are few concrete policy implications, except for a general sense that more transparency would be good. Instead, the book succeeds at an intermediate level, with informed

BETTER UNDERSTANDING OF THE RELATIONSHIP BETWEEN SECRECY AND SECURITY WILL BE CRUCIAL IN COMING YEARS AS THE NATION SEEKS TO BUILD A SOCIETY THAT IS BOTH OPEN AND SECURE.

description and thoughtful discussion of particular practical problems.

In particular, Roberts does not effectively explain how transparency can be both increasing and decreasing at the same time. Early on, he describes transparency on the march, but in the remainder of the book he describes transparency in eclipse. How can both be true?

This apparent contradiction can be explained. On the one hand, the volume of information available to the public has increased enormously because of computerization. A simple FOIA request today might garner thousands or even millions of emails or data fields, on a scale unimagined when the law was created. In ways that are threatening to government officials, a leaked document today can be uploaded instantly to a blog and then quickly reach the mainstream media. At the same time, however, the categories of information subject to secrecy rules also are increasing. Together, these two factors can explain the anguish felt by transparency advocates and government officials alike. Advocates note the new categories of secrecy and lament the loss of access. Officials note the ways in which technology hastens the spread of secrets. Both sides of the debate see how they are worse off than before. Both are correct that they have lost something compared to what existed previously.

Roberts also falls short in clarifying the interplay between secrecy and security. Early on, he accurately describes how the 9/11attacks have bolstered individuals and groups who want to keep secrets in the name of national security. In response, as a transparency advocate, Roberts makes the vague claim that "In the long run, it may be a policy of openness rather than secrecy that best promotes security." He says, for instance, that greater transparency may reveal the weaknesses in new homeland security programs and lead to their strengthening.

Roberts's hope that openness best promotes security has in fact become a major theme for security researchers in recent years. Most of them are active in computer security, where there is an oft-used maxim that "there is no security through obscurity." This maxim is most persuasive in the context of open-source software projects. In such settings, when a security flaw is publicized, a corps of software programmers can leap into action to write an effective patch. Furthermore, the publicity alerts users of the software to the problem and encourages them to protect their own systems once a patch is developed. In short, publicity helps the defenders (the software writers and system users) but does not tell much to the attackers.

The difficulty is that sometimes publicity helps the attackers but not the defenders. The maxim that favors secrecy is "loose lips sink ships." Revealing the path of the convoy helps would-be attackers but does nothing to aid defenders. Both "no security through obscurity" and "loose lips sink ships" cannot simultaneously be true. Instead, it is a key research task, including for transparency advocates such as Roberts, to determine the conditions under which disclosure is likely to help or hurt security. In other writings, I have tried to contribute to that research project, especially by identifying the costs and benefits of disclosure to attackers and defenders in various settings. One key theme is that secrets work well against a first attack, when the attackers might fall for a trap. Secrets work much less well against repeated attacks, such as when a hacker can try repeatedly to find a flaw in a software program or system firewall.

Better understanding of the relationship between secrecy and security will be crucial in coming years as the nation seeks to build a society that is both open and secure. By so ably documenting the current trends toward both openness and secrecy, Roberts has provided a crucial underpinning for that debate.

Peter P. Swire (peter@peterswire.net) is the C. William O'Neill Professor of Law at the Moritz College of Law, Ohio State University, and a senior fellow at the Center for American Progress in Washington, DC. He served as the Chief Counselor for Privacy in the U.S. Office of Management and Budget from 1999 to 2001.