Steven Aftergood

National Security Secrecy: How the Limits Change

AS A NATION, WE SEEM TO BE OF TWO MINDS ABOUT SECRECY. WE know that government secrecy is incompatible with democratic decision-making in obvious ways. By definition, secrecy limits access to official information, thereby impeding public participation in the deliberative process and inhibiting or preventing the accountability of government officials for their actions. Yet there is a near universal consensus that some measure of secrecy is justified and necessary to protect authorized national security activities, such as intelligence gathering and military operations, to permit confidential deliberations in the course of policy development, to secure personal privacy, and for other reasons.

Reconciling these conflicting interests is an ongoing challenge. A stable secrecy policy is hard to achieve since the proper boundaries of official secrecy cannot be clearly articulated in the abstract and tend to shift over time. In practice, decisions to restrict information seem to depend on prevailing security considerations (secrecy is more pronounced in time of war), official predispositions (some political leaders favor secrecy more than others), and public attitudes and expectations.

In recent years, a large and growing number of public interest organizations and professional societies have turned their attention to government secrecy, identifying it as an obstacle to achieving their own objectives. In fact, there are at least two entire coalitions of organizations devoted to combating secrecy: Openthegovernment.org and the

Research for this paper was supported by grants from the Foundation to Promote Open Society, the HKH Foundation, the CS Fund, the Stewart R. Mott Foundation, and the Rockefeller Family Fund.

Sunshine in Government Initiative. (Sometimes they collaborate too, in a sort of metacoalition.)

These professionally and politically diverse groups are united by the perception that secrecy has escalated to the point of dysfunction. On that point, there is not much disagreement. The 9/11 Commission, for example, concluded in its final report that excessive secrecy left the nation needlessly ill-prepared for the threat of terrorism, that it obstructed communications within the government, and that it left the public in the dark on matters of vital interest and importance (*The 9/11 Commission Report* 2004: 341, 410).

One basic premise of the critics of government secrecy is that too much information is classified and withheld from the public in the name of national security, and that this has undesirable effects on public policy and on public discourse. But a second basic premise is that it is possible to do something about that. These organizations, including my own, do not simply want to protest against improper secrecy but to correct it. And to a remarkable extent, the secrecy system lends itself to such corrective efforts through various mechanisms that will be described below.

But first, a bit of background.

The national security secrecy system that took shape in the early Cold War period has persisted with surprising continuity up to the present day. Although President Barack Obama issued a new executive order in December 2009 establishing his own version of the secrecy system, the Obama order is structurally and functionally nearly identical to its predecessors. Like them it has three levels of classification of increasing sensitivity; like them classification is defined by a presumption of damage to national security that would result from disclosure; and like them it is regulated by a so-called need to know, which means that only those who have a recognized requirement for the information can gain authorized access to it. When the Obama order came out, one could not help noticing that its number—Executive Order 13526—was a simple rearrangement of the number of President Ronald Reagan's 1982 classification order: Executive Order 12356. And their commonalities go much deeper than that.

It should be acknowledged that the United States has the most open government in the world. No other country publishes a comparable avalanche of government information on a daily basis. Paradoxically, however, one could also say that the United States has the most secretive government in the world, at least in the sense that no one else generates a comparable profusion of secret data, including tens of thousands of new national security secrets each day. This is because no other country has a military and intelligence infrastructure anywhere near the size of ours.

In any case, the secrecy system does not exist in some kind of abstract isolation. It is an ordinary bureaucratic artifact that is subject to pressure on many levels—political, legal, sociological, international, and others. It is constantly undergoing changes due to press reporting and leaks (unauthorized disclosures), budget appropriations and congressional oversight, Freedom of Information Act requests and lawsuits, and foreign government disclosures, errors, whistleblowers, financial pressures, and—not least important– an ideological or tactical preference for disclosure—or the opposite—on the part of senior officials.

These pressures, discussed below, regularly induce changes in the scope of secrecy. Up to a point they can be harnessed deliberately to achieve specific disclosure goals.

INVESTIGATIVE REPORTING AND UNAUTHORIZED DISCLOSURES

It is hard to say what the single most important mechanism for combating or overcoming national security secrecy might be, but certainly the role of the news media is essential.

We celebrate the contributions of investigative reporters who bring us vital, often disturbing information from across the boundary of official secrecy. Hardly a day goes by without a reference in the national media to a classified document or to classified information that has been disclosed to a reporter, usually on condition of anonymity.

The astonishing fact is that our government, despite its vast secrecy apparatus, is basically susceptible to the process of investigative report-

ing. That is not something to be taken for granted. We know there are societies so tightly sealed or so politically unstable or insecure that even the most determined journalists are helpless to penetrate them, and they risk their lives by attempting to do so.[1] But that is not the situation we are in—far from it. It may not be easy, but in our society it is perfectly possible to do the work of probing into secret government activities and to return safely to the public domain with a story to tell.

My own project at the Federation of American Scientists started in the early 1990s when I obtained a series of classified documents about a classified Defense Department program to develop a nuclear reactor-driven rocket, code-named Timber Wind. I publicized and distributed the documents. I also filed a complaint with the Pentagon's inspector general, arguing that the program had been improperly established as a highly classified special access program. Ultimately the inspector general agreed that it was overclassified (Timber Wind 1992). I took this experience as a general confirmation of the two premises mentioned above: both that there is a problem with excessive secrecy, and that it is possible to do something about it. Not only did I not get in trouble for soliciting, receiving, and disseminating classified information in this case, but the Timber Wind program managers were rebuked for misusing their classification authority, and ultimately the program was canceled.

I do not mean to exaggerate my own humble accomplishments. My point is more like the opposite: uncovering government secrets is not an extraordinarily difficult task in our society today. It is quite feasible even for someone with no training in journalism, no influential publisher, and no name recognition or mass following.

It is true that under some circumstances, the unauthorized disclosure of classified information to the press or anyone else is a violation of the law. But only three people have ever been convicted of such a crime in a nonespionage case. (These were Samuel L. Morison in 1985, Lawrence A. Franklin in 2005, and ~~Shabtai~~ Leibowitz in 2010. Other leak prosecutions are pending.) "Given that literally thousands of press leaks have occurred in recent years," a 2002 analysis by a Central Intelligence Agency official complained, "it is clear that current laws do

not provide an effective deterrent to leakers or to journalists and their media outlets that knowingly publish classified information" ("Leaks" 2002). This may be good or bad, depending on one's perspective and on the information in question, but it is a testament to the remarkable absence of external legal constraints on the press.

In any case, it is important for those who value the uniquely robust freedom of the press that we have in this country, which extends even to the publication of national secrets, to recognize the enabling conditions that make it possible. The First Amendment is not some transcendent ideal, and it is not self-actualizing or self-enforcing. Its effectiveness as an instrument of liberty depends on a set of social, political, legal, and moral norms that are absent even in some other democracies (see Pepper 2010).

Notably, press freedom also depends on a bedrock of security considerations, including a capacity to protect genuine national security secrets—a dependence that is perhaps not acknowledged frequently enough by those of us who seek to reduce or to counter official secrecy. In a world of violent conflict, a nation that was completely unable to keep a secret would not be able to defend the First Amendment or anything else for very long. So in some paradoxical but real sense, one might say that freedom of the press is both at odds with government secrecy and also contingent on the national security that secrecy helps to support, at least when it is properly used.

FOIA'S CENTRALITY

The Freedom of Information Act (FOIA) is one of the most important levers that the public has for challenging government secrecy. It gives legal standing to "any person" to seek government records, and it requires the government to provide those records unless they fall in an exempted category. It is a law that has been employed with impressive results by the American Civil Liberties Union, the Associated Press, the Electronic Frontier Foundation, the National Security Archive, and many other organizations and individual requesters. Much of the record of Bush administration policy on interrogation and torture of suspected enemy

combatants that is in the public domain is there thanks to the dogged and effective use of FOIA by the American Civil Liberties Union (ACLU).

But the real power of the act may be revealed in more mundane cases that are not necessarily the subject of national controversy. "Countless media outlets, government watchdog groups and individual Americans have used the Freedom of Information act to obtain important information on how—and how well—the government operates," observes the Sunshine in Government Initiative, which has collected hundreds of news stories that made use of the FOIA.[3]

In many FOIA cases, the mechanism that is needed to shift the limits of knowledge is: just ask. Sometimes that is all it takes.

In one FOIA case, I asked the National Reconnaissance Office (NRO)—the intelligence agency responsible for overhead surveillance and spy satellites—for a copy of certain budget documents, but the agency refused to provide them. I appealed, and the NRO denied the appeal. So I took the matter to court, and although I am not an attorney, I managed to present a legal argument that the judge found persuasive, and he ordered the NRO to provide the requested records. In other words, Judge Reggie Walton of the D.C. district court ruled that a U.S. intelligence agency was wrong and that a private individual (myself), who did not even have a lawyer, was right (Memorandum Opinion 2006). This was not the outcome that a cynic would have predicted. In fact, it set a sharp limit on my own capacity for cynicism about the possibilities of change. It could only be accomplished because of the power of that extraordinary law, the FOIA.

It should be added that the FOIA does not always work well, particularly for those who are not prepared to litigate their requests. And even for those who do litigate, the FOIA can be a double-edged sword. If you do not know what you are doing, if you do not have a legally compelling argument, or if you are simply unlucky, not only will you lose in court, but you may leave behind a trail of legal wreckage and bad precedents that will make life harder for those requesters who come after you.

In a bit of promising news, the John S. and James L. Knight Foundation announced in January 2010 that it will dedicate $2 million in grants to support Freedom of Information Act litigation. This kind of

aid should help to ensure that FOIA remains a vital and vibrant mechanism for shifting the limits to knowledge (Curnow 2010).

ERRORS

Another significant driver of change in official secrecy is the inadvertent, unintentional disclosure of controlled information. To a surprising extent, the secrecy system is porous and accident prone, failing to provide the protection that is its reason for existence. With approximately 2.5 million Americans holding security clearances, and tens of millions of new secret records generated each year, there was no way the secrecy system was ever going to be watertight or foolproof. But with the growing dominance of electronic records in the last decade or two, inadvertent disclosures—which are different than intentional leaks—seem to have steadily increased. You usually cannot get the things you really want through such errors, but it's often possible to get all kinds of things you were not necessarily looking for.

In December 2009, it emerged that the Transportation Security Administration had published online a security manual describing the detailed procedures for screening airline passengers and luggage. The manual, which was protected by law as Sensitive Security Information or SSI, also revealed, at least by implication, how those procedures could be circumvented. The document had been redacted by TSA—that is, the sensitive parts were blacked out—but officials performed the redaction incorrectly so that the censored portions could be readily uncovered (Ross and Hosford 2009).

In June 2009, the Government Printing Office (GPO) published a restricted, 267-page draft U.S. government document describing U.S. civilian facilities where nuclear weapons-related research was being carried out. This document, which was to be submitted by the United States to the International Atomic Energy Agency in fulfillment of treaty obligations, had been mistakenly forwarded to the GPO and it had naturally published it, since that is what the GPO does. A firestorm of controversy erupted, and after everyone on the planet who might conceivably have wanted a copy already possessed one, the document was removed from the GPO website (Warrick 2009).

It is clear that the limits to knowledge imposed by national security secrecy are themselves limited and are often undermined by human error. Sometimes one may be grateful for that, and other times not.

William Safire, the late *New York Times* columnist and sometime aide to President Richard Nixon, once wrote that "authority always errs on the side of concealment, requiring subjects to strike a balance by erring on the side of revelation (Safire 1992: 205)." This is a clear and simple principle, jauntily expressed. But from my point of view it is not very good advice, because in many cases the errors of disclosure do not balance or correct the errors of secrecy.

With some frequency, I discover erroneous or questionable disclosures that I feel constrained not to publicize. (Up to a point this calls into question the first of my working premises mentioned above—that too much information is controlled and withheld from the public. That premise should perhaps be modified to say that the boundaries of the secrecy system are incorrectly drawn.)

Last year, I found a copy of a 474-page U.S. Army manual on the training of Special Forces snipers. It described the missions, techniques, skills, and training of a military sniper. It was not intended for public release, but it was inadvertently disclosed anyway—at least if you knew where to look for it. And though my organization provides an online library of Army field manuals and other doctrinal materials, I did not see any good reason to make it widely available on our website.

Similarly, I obtained another Army manual with hundreds of pages on the proper operation, maintenance, and use of shoulder-fired munitions, a type of weapon that could potentially be used against civilian targets in terrorist scenarios. I did not think that disclosure of this document would balance the nondisclosure of secret records that were wrongly withheld, and so this is another case where I chose to exercise self-restraint and to refrain from publishing the document.

The basic point is that the secrecy system is error prone. And the larger and more prolific it becomes in generating and disseminating secrets, the more errors one is likely to discover. Those errors can shift the limits to knowledge, whether for good or ill.

OFFICIAL INVESTIGATIONS AND CONGRESSIONAL OVERSIGHT

One of the most powerful instruments for breaking down classification barriers and releasing secret information into the public domain is the kind of focused official investigation that is periodically undertaken to address matters of unusual urgency or public controversy. Information that was originally disclosed by the Church committee investigations of intelligence activities in the mid-1970s is still finding its way into new books on intelligence and national security. Likewise, the 9/11 Commission catalyzed a massive release of classified records of the sort that the public almost never sees, and would never be able to obtain through FOIA lawsuits or other normal channels.

And for that reason, it is regrettable that Congress could not rouse itself to establish a commission of inquiry into the detention, interrogation, and surveillance practices of the war on terrorism. Such a commission was proposed last year by Senator Patrick Leahy, but except for a single Senate hearing ("Getting to the Truth" 2009), it never went anywhere. The commission would probably not have resolved any of the continuing disputes over counterterrorism policies, but it almost certainly would have significantly enriched the public record.

However, it does not take an extraordinary, once-in-a-generation commission to have this kind of effect. The normal friction that accompanies congressional oversight very often serves as a driver of public disclosure. Certainly that was true with the congressional joint inquiry into 9/11, which returned a trove of interesting information and records and saw that they were declassified. It is also true of the routine process of congressional oversight of intelligence and national security, including the submission of detailed budget requests to Congress, and the resulting authorization and appropriations reports, which are often the first place that new knowledge is disclosed. (I always try to review the published record of significant congressional hearings in my areas of policy interest, because they sometimes include official answers to "questions for the record" that are extremely informative and interesting. Although they do not usually appear until six months or a year after the original hear-

ing, they often introduce valuable new information into the public domain.)

INTERNAL EXECUTIVE BRANCH OVERSIGHT

There may be a tendency to dismiss the value of internal executive branch oversight as anemic and compromised by a conflict of interest. Sometimes it is. But in practice, some of the most effective checks and balances on government operations, including new public disclosures of formerly secret information, take place through the process of internal oversight.

Reports of agency inspectors general have frequently generated news not only because of their policy conclusions and recommendations, but also because of what they reveal about the conduct of national security activities. If one wants to learn about irregularities in the FBI's use of so-called national security letters, for example, the place to start is the work of the Justice Department inspector general.

Another surprising and unexpected fact is that internal oversight provides one of the most consistently effective remedies to excessive secrecy within the executive branch itself. An entity called the Interagency Security Classification Appeals Panel (ISCAP) has overturned more executive branch classification decisions than any court or legislative action has.[4] Since it was established in 1995 it has ordered the declassification in whole or in part of the majority of documents that have been presented for its review—against the objections of the originating agency. That is a remarkable record. Judicial review of classified documents in FOIA litigation does not come near that kind of performance.

Based on such experiences, efforts to strengthen and thicken internal oversight within the executive branch have the potential to pay tremendous dividends in terms of correcting classification errors and shifting the limits to knowledge in the direction of greater disclosure. Internal oversight may also be more palatable to some agencies that would tend to resist intervention by Congress or the courts.

THE IMPORTANCE OF LEADERSHIP

Some of the most dramatic and far-reaching changes in the limits to public knowledge of national security matters are directly attributable

to individual leadership—both at the top of the executive branch and throughout the agencies. The simple fact is that some officials favor openness and disclosure—either as a matter of principle, or for tactical political reasons—and some are hostile to it.

One of the relatively few success stories in the history of efforts to reduce national security secrecy is the Department of Energy (DOE) "openness initiative" that was undertaken by Energy Secretary Hazel O'Leary beginning in December 1993. For a variety of reasons, including controversy over human radiation experiments, mounting public cynicism over environmental contamination at government facilities, and other concerns, Secretary O'Leary decided that openness was both good policy and good politics. She turned her department upside down to make it happen. For the first time, a complete record of U.S. nuclear explosion tests was published, detailed histories of the production of plutonium and highly enriched uranium were prepared and released, the scope of DOE classification was narrowed, and prohibitions were put in place against classifying environmental, health and safety information.

A DOE spokesman at the time borrowed a line from an old cigarette commercial and said that the Department of Energy was "going to classify less, and enjoy it more." And for a while, that's what it did.

Today, the Obama administration's often-declared support for openness as a guiding principle provides an opportunity to test the importance of presidential leadership in shifting the limits to knowledge. Although there have already been some interesting achievements and some unfortunate setbacks, there is reason to believe that the most important developments in open government are still to come.

Slowly but steadily, and in modest but important ways, government agencies are starting to integrate the administration's instructions on increased transparency into their own operations and training, and they are building what has the potential to become a new infrastructure of openness as well as a basic change in attitude and orientation toward public disclosure.

For example, an Army official at a government conference last year interpreted the new Obama policies for other Army personnel

by explaining that we are entering "a new era of open government" ("Presidential, Congressional, and Policy Changes" 2009)." He advised the Army attendees that there will be an "increased emphasis on FOIA programs" and that the "[FOIA] requester is not an adversary." This presentation, which was not staged for public consumption, may have signified a larger transformation in the bureaucracy. Never mind that FOIA proceedings are often in fact quite adversarial. The official was telling his colleagues and his subordinates that FOIA requesters and responders are part of the same process, and that it is incumbent on all sides to make the process work. This is not a message that has been heard for a long time. If that message is successfully transmitted and absorbed throughout the government, it could have far-reaching, positive implications for public access to government information.

One of the Obama administration's most promising innovations is what it calls the Fundamental Classification Guidance Review. It is a requirement for each classifying agency to systematically and impartially review its classification policies in order to identify and eliminate obsolete classification practices. The review requirement was imposed in the president's recent executive order, and it is to be completed within two years. When the Department of Energy did something similar in 1995, it led to a real reduction in the scope of classification and the release of a tremendous amount of material.

The new fundamental review requirement is "the most important effort to address this problem [of overclassification]," said William H. Leary of the National Security Council, who helped draft the Obama executive order on classification policy. "These reviews can be extremely important in changing the habits and the practices of classifiers throughout government" (Leary 2010).

We will see whether or not that turns out to be the case, and whether the limits to knowledge can be shifted in this way. But experience suggests that it is worth a try (Aftergood 2009).

CONCLUSION

To an important extent, the limits to knowledge in matters of national security policy will yield to the pressures of news gathering, public

inquiry, and the other factors noted above. While the official limits may initially be set in an arbitrary or mistaken manner, they can often be shifted over time by an engaged and determined public, and even by some of its individual members.

"No information may remain classified indefinitely," President Obama declared in his 2009 executive order. Taken at face value, this means that all of the formal limits to public knowledge of national security matters that are now in place are transient and must sooner or later give way.

NOTES

1. The Committee for the Protection of Journalists provides current statistics on the number of reporters around the world who have been imprisoned or killed in the course of their work. See <www.cpj.org>.
2. Even in democratic India, some users of that country's freedom of information law have been hospitalized or murdered for their efforts. See Pepper (2010).
3. See "The FOIA Files" <http://www.sunshineingovernment.org/stories/>. Another compilation of significant FOIA releases obtained by the Electronic Privacy Information Center may be found at <http://epic.org/open_gov/foiagallery2010.html>.
4. See the Interagency Security Classification Appeals Panel website at <http://www.archives.gov/isoo/oversight-groups/iscap/index.html>.

REFERENCES

Aftergood, Steven. "Reducing Government Secrecy: Finding What Works." *Yale Law and Policy Review* 27:2 (Spring 2009): 399-416.

Curnow, Charlie. "Knight Foundations Donates $2 Million to Freedom of Information Groups." *The Daily Tell*, January 7, 2010 <http://www.thedailytell.com/2010/01/knight-foundation-donates-2-million-to-freedom-of-information-groups/>.

Executive Order 13526. "Classified National Security Information." December 29, 2009 <http://www.fas.org/irp/offdocs/eo/eo-13526.htm>.

"Getting to the Truth through a Nonpartisan Commission of Inquiry." Hearing before the Senate Judiciary Committee. March 4, 2009 <http://www.fas.org/irp/congress/2009_hr/truth.html>.

"Leaks: How Unauthorized Media Disclosures of U.S. Classified Intelligence Damage Sources and Methods." Central Intelligence Agency memorandum, April 24, 2002 <http://www.fas.org/irp/cia/product/leak-report-supp.pdf>.

Leary, William H. Panel discussion on national security classification sponsored by the Collaboration on Government Secrecy, Washington College of Law, American University, January 20, 2010.

Memorandum Opinion in *Steven Aftergood v. National Reconnaissance Office.* D.C. District Court Case No. 05-cv-1307 (RBW), July 24, 2006 <http://www.fas.org/sgp/foia/nro-cbjb/rbw072406.pdf>.

The 9/11 Commission Report. Final Report of the National Commission on Terrorist Attacks upon the United States. Washington, D.C., 2004.

Pepper, Daniel. "In India, Deadly Backlash Against Freedom of Information Activists." *Christian Science Monitor,* March 10, 2010.

"Presidential, Congressional, and Policy Changes to the FOIA." Presentation to the Army FOIA, Privacy and Records Management Conference. November 2009 <http://www.fas.org/sgp/othergov/dod/army-foia.pdf>.

Ross, Brian, and Matt Hosford. "Massive TSA Security Breach as Agency Gives Away Its Secrets." ABC News, December 8, 2009 <http://abcnews.go.com/Blotter/massive-tsa-security-breach-agency-secrets/story?id=9280503>.

Safire, William. *The First Dissident: The Book of Job in Today's Politics.* New York: Random House, 1992.

The Timber Wind Special Access Program. Department of Defense Inspector General Audit Report No. 93-033. December 16, 1992 <http://www.fas.org/sgp/othergov/dod/tw.pdf>.

Warrick, Joby. "List of U.S. Nuclear Sites Inadvertently Posted Online." *Washington Post*, June 3, 2009.