GOVERNMENT SECRECY AND KNOWLEDGE PRODUCTION: A SURVEY OF SOME GENERAL ISSUES

Steven Aftergood

Introduction

Secrecy and the production of knowledge are, to all appearances, in conflict. Certainly the self-understanding of the scientific enterprise asserts the essential importance of the open exchange of information, which is the very opposite of secrecy. According to one of the nation's leading scientific societies, "The basic function of the scientific community is the advancement of knowledge, including its clarification, interpretation, diffusion, and evaluation."[1]

If science pursues the advancement of knowledge generally, including the diffusion of that knowledge, secrecy emphasizes the value of *differential* knowledge: If I can prevent you from knowing something that I know, I may be able to derive benefits in terms of military or economic advantage from the secret knowledge that I hold. By doing so, however, I may at some point inhibit my own ability to gain new knowledge. This paper briefly surveys the national security classification system, and considers several instances where official secrecy has intersected with the production of technical knowledge—for good or ill.[2]

An Overview of the National Security Classification System

> Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national interest has

---

[1] John T. Edsall, *Scientific Freedom and Responsibility* A Report of the AAAS Committee on Scientific Freedom and Responsibility (Washington, DC.: American Association for the Advancement of Science, 1975), p. x.

[2] There is a sizable literature on the conflict between science and national security that I will not even attempt to summarize. See, for example: Harold C. Relyea, *Silencing Science: National Security Controls and Scientific Communication* (Norwood, NJ: Ablex Publishing, 1994); and Herbert Foerstel, *Secret Science: Federal Control of American Science and Technology* (Westport, CT: Praeger Publishers, 1993). On national security secrecy generally, see Sen. Daniel P. Moynihan (chair), *Report of the Commission on Protecting and Reducing Government Secrecy*, U.S. Government Printing Office, March 1997 <http://www.fas.org/sgp/library/moynihan/index.html>.

> required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations.[3]

Government imposes restrictions on information for a variety of reasons—to protect personal privacy, to preserve the confidentiality of law enforcement investigations and diplomatic initiatives, and to prevent "damage to national security," an objective whose definition is fluid and to a certain degree subjective. This latter function, the use of controls on information in order to protect national security, is the purpose of the national security classification system. The current classification system is governed by Executive Order 12958, issued by President Clinton in April 1995. (A separate, but parallel, classification system is rooted in the Atomic Energy Act of 1954 and applies solely to "atomic energy information.")

Information that is owned by, produced for, or otherwise controlled by the U.S. government may be "classified" (i.e., withheld from disclosure) if it concerns one of the following categories:[4]

- military plans, weapons systems, or operations;
- foreign government information;
- intelligence activities (including special activities), intelligence sources or methods, or cryptology;
- foreign relations or foreign activities of the United States, including confidential sources;
- scientific, technological, or economic matters relating to the national security;
- United States Government programs for safeguarding nuclear materials or facilities; or
- vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

Even information that does fall into one of these categories is not supposed to be classified unless a responsible official determines that its disclosure "reasonably could be expected to result in damage to the national security" and the official can identify or describe that damage. Further-

---

[3] Executive Order 12958, "Classified National Security Information," 60 *Federal Register 19825*, April 20, 1995.

[4] "Classified National Security Information," section 1.5.

more, "Basic scientific research information not clearly related to the national security may not be classified," the Order directs.[5]

That is the theory; the actual practice is considerably more complex.

One degree of complexity arises from the enormous size and volume of the secrecy system. The number of government officials who are authorized to designate information classified was most recently reported to be 4,420.[6] Inevitably, the expectation of what might result in damage to national security will vary considerably among these thousands of individuals, and it is possible to find startling discrepancies in the classification and declassification practices of various agencies.[7] The total number of classification actions reported in the most recent year alone was over 5.7 million. "How much classified information is contained in the total universe of classified information?" That is a question that "we cannot definitively answer," the Information Security Oversight Office reported to the President. Nevertheless, it is clear that there are well in excess of one billion pages of classified documents that are over 25 years old which have been deemed historically valuable.

Three Categories of Secrecy

A different sort of complexity has to do with the subjective aspect of the classification system and its resulting susceptibility to abuse. In the actual practice of national security classification, it is possible to discern three general categories: genuine national security secrecy, political secrecy, and bureaucratic secrecy.[8]

---

[5] "Classified National Security Information," section 1.8b

[6] Information Security Oversight Office, "1996 Report to the President," National Archives and Records Administration, 1997 <http://www.fas.org/sgp/isoo/isoo96.html>.

[7] The essentially arbitrary, or at least subjective, nature of the classification process has encouraged one research strategy sometimes used by historians and others, i.e., requesting the declassification of the same document from multiple agencies, since different agencies will often release (and withhold) different portions of a particular classified document.

[8] This discussion is borrowed from an earlier paper: "Secrecy and Accountability in U.S. Intelligence," prepared for the Center for International Policy, October 1996 <http://www.fas.org/sgp/cipsecr.html>.

Genuine national security secrecy pertains to that information which, if disclosed, could actually damage national security in some identifiable way. Without attempting to conclusively define "national security" or "damage," common sense suggests that this category would include things like design details for weapons of mass destruction and other advanced military technologies, as well as those types of information that must remain secret in order for authorized diplomatic and intelligence functions to be performed.[9] This, of course, is the only legitimate form of national security secrecy.

Political secrecy refers to the deliberate and conscious abuse of classification authority for political advantage, irrespective of any threat to the national security. This is the least common of the three categories, but the most dangerous to the political health of the nation. Perhaps the most extreme example of political secrecy historically was the classification of CIA behavior modification experiments on unknowing human subjects, as in the MKULTRA program. To guarantee the permanent secrecy of this activity, most MKULTRA records were destroyed in the early 1970s.[10]

An exceptionally blunt expression of political secrecy is contained in a 1947 Atomic Energy Commission memorandum which instructs that

> It is desired that no document be released which refers to experiments with humans and might have adverse effect on public opinion or result in legal suits. Documents covering such work . . . should be classified "secret."

This memorandum itself remained classified Secret until its declassification in 1994.[11]

The third category is what may be called *bureaucratic secrecy*. As classically described by Max Weber, this has to do with the tendency of all organizations to limit the information that they release to outsiders so as to control perceptions of the organization. Bureaucratic secrecy appears

---

[9] President Nixon's Executive Order 11652 gave the following examples of what would constitute "exceptionally grave damage" to national security: armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

[10] See, generally, John Marks, *The Search for the 'Manchurian Candidate': The CIA and Mind Control* (New York: Times Books, 1979).

[11] "Medical Experiments on Humans," Memorandum from O.G. Haywood, Jr. to Dr. Fidler, Atomic Energy Commission, April 17, 1947, attached herewith (Appendix A).

to be the predominant factor in current classification practice, accounting, in my opinion, for the majority of the billions of pages of classified records throughout government.

There is inevitably a subjective factor involved in assigning a particular unit of information to one of these three categories of secrecy. The borders of the three categories may sometimes be blurred in practice. Furthermore, information that falls in one category at one moment will often belong in another category at some later date. Responsible classification management—i.e., the elimination of all but genuine national security secrecy—therefore depends to a large degree on the good judgment and the good will of the classification officials themselves.

When responsible classification management fails, or when classification authority is abused, the result is . . . pathological secrecy.

Pathological Secrecy

In the best of cases, secrecy undercuts the possibility of peer review and oversight. In the worst of cases, secrecy will be applied far out of proportion to any requirements of national security and will lead to bad policy, sometimes on a large and expensive scale. There are several instances in the last decade in which secrecy has caused or contributed to the failure of multi-billion dollar technology programs.

The Navy's A-12 attack aircraft program is something of a paradigm of a secret program run amok. The A-12 was a "special access" program, which means that access to information about the program was strictly limited using controls above and beyond those applied to other classified information. Because of these stringent controls on access, oversight was inhibited and officials were slow to learn that the program could not possibly accomplish its goals, resulting in its cancellation in 1991 after the expenditure of some $2.7 billion dollars. "The fact that it was a special access program, and the fact that there were limited clearances granted to oversight individuals to look at the program certainly were contributing factors" in the program failure, according to the Department of Defense Inspector General.[12] Secrecy was likewise a contributing

[12] House Armed Services Committee, hearing on "The Navy's A-12 Aircraft Program," 101 Congress, December 10, 1990 [HASC No. 101-84], p. 88.

factor in the failure of several other large special access programs including the $3.9 billion Tri-Service Standoff Attack Missile (TSSAM)[13] and the Tacit Rainbow anti-radar missile.[14]

Abuses of classification authority on a smaller scale are even more common. The decision to classify the TIMBER WIND nuclear rocket propulsion program as an unacknowledged special access program "was not adequately justified," according to a 1992 Department of Defense Inspector General audit.[15] The Strategic Defense Initiative Organization "continued to safeguard its association with the technology for reasons that were not related to national security." The program was terminated within two years after its existence was disclosed (without authorization) to the public.[16]

Alert members of Congress eventually began to detect a pattern and a common thread in such failures. As the House Armed Services Committee put it:

> The Committee believes that the Special Access classification system has progressed beyond its original intent, and that *it is now adversely affecting the national security* it is intended to support.[17]

While oversight of the most highly classified special access programs seems to have improved in last few years, anecdotal reports indicate a continuing problem with pathological secrecy.

---

[13] Bradley Graham, "Missile Project Became a $3.9 Billion Misfire," *The Washington Post*, April 3, 1995, page A1. "Inhibiting wider scrutiny of TSSAM was its highly classified nature . . . Northrop's Kresa said the secrecy surrounding this and other cruise missile projects complicated his company's attempts to hire qualified people . . . ."

[14] On so-called "black programs" generally, see Tim Weiner, *Blank Check: The Pentagon's Black Budget* (New York: Warner Books, 1990).

[15] Department of Defense Inspector General, "The TIMBER WIND Special Access Program," Report Number 93-033, December 16, 1992. "Pentagon Audit Blasts SDI Nuclear Rocket Classification," by Joseph Lovece, *Defense Week*, January 11, 1993.

[16] William J. Broad, "Rocket Run by Nuclear Power Being Developed for 'Star Wars'," *New York Times*, April 3, 1991; R. Jeffrey Smith, "U.S. Developing Atom-Powered Rocket," *Washington Post*, April 3, 1991; "DoD Cancels Plans for Nuclear Rocket," by Vincent Kiernan, *Space News*, May 17-23, 1993.

[17] House Armed Services Committee, "National Defense Authorization Act for Fiscal Years 1992 and 1993," Report No. 102-60, May 1991, p. 101.

> [Philip] Odeen [chairman of the 1997 National Defense Panel] confirmed that a number of secret weapons were not used in the Persian Gulf war either because their capabilities couldn't be revealed to commanders—or because they were offered too late in the conflict. "Guys came to us saying they had something that would win the war," one wartime commander told us. "When I asked what it was, they'd say, 'I can't tell you,' or 'I can't reveal the effects,' or 'I can't tell you how it would work with other systems.' We told them to get the hell out."[18]

Of course, not all secret programs are failures. In some important cases, secrecy may actually have contributed to success.

CORONA: A Secret Success Story

Secrecy is not absolutely incompatible with the advancement of scientific and technical knowledge. Some of the most dramatic technological breakthroughs have been achieved under a rigorous framework of official controls on information. The development of the atomic bomb is one example. The United States' first satellite reconnaissance program, codenamed CORONA, is another.[19]

CORONA, which began in 1960 and continued until 1972, was a joint effort of the Central Intelligence Agency, the Advanced Research Projects Agency, and the Air Force. To say that CORONA revolutionized intelligence and space exploration would be no exaggeration. According to an official history of the program:

> The totality of CORONA's contribution to U.S. intelligence holdings on denied areas and to the U.S. space program in general is virtually unmeasurable. Its progress was marked by a series of notable firsts: the first to recover objects from orbit, the first to deliver intelligence information from a satellite, the first to produce stereoscopic satellite photography, the first to employ multiple reentry

---

[18] James R. Asker, ed., "Washington Outlook," *Aviation Week & Space Technology* 147 (October 13, 1997): 21. See also a discussion of the emergence of the Stealth Fighter from classified status, which posed the question: "If the very existence of the aircraft is to be protected at the expense of using it, what is the purpose for having such a weapon?" Jim Cunningham, "Cracks in the Black Dike: Secrecy, The Media, and the F-117A", *Airpower Journal* (Fall 1991): 32. <http://www.cdsar.af.mil/apj/cunn.html>.

[19] See also the chapter by John Cloud, this volume.

> vehicles, and the first satellite reconnaissance program to pass the 100-mission mark.[20]

Most important of all, CORONA permitted an empirical assessment of Soviet military capabilities—a field previously dominated by worst-case thinking.

On its way to ultimate success, however, CORONA suffered a series of daunting setbacks that would have doomed another program. The first dozen launches were all failures. Of the first 30 missions, only 12 were productive.[21] Although several of the launch failures (and some of the successes) were noted in the press at the time, the overall secrecy of the program, together with the urgent need for its success, helped shield CORONA from the political consequences of its recurring failures and nurtured the program to a successful conclusion.

A View from Industry

One might suppose that defense contractors would enthusiastically support the secrecy system, since they are the beneficiaries of several billion dollars of secret government largesse each year. But that is not necessarily the case.

The legendary Lockheed Skunk Works, the most famous of the defense contractors specializing in classified programs, has also offered outspoken criticism of secrecy policies. Ben R. Rich, who participated in the trailblazing Skunk Works projects to develop the U-2 spy plane, the SR-71 Blackbird, and the F-117 Stealth Fighter, wrote:

> A classified program increases a manufacturer's costs up to 25 percent . . . In the past, the government has slapped on way too many security restrictions in my view. Once a program is classified secret it takes an act of God to declassify it . . . What was secret in 1964 often is probably not even worth knowing about in 1994. I would strongly advocate reviews every two years of existing so-called black programs either to declassify them or eliminate them entirely. . . .
>
> Secrecy classifications are not inconsequential but a burden to all and horrendously expensive and time-consuming. If necessarily in the national interest, these expenses and inconveniences are worthwhile. But we ought to make damned

---

[20] Kenneth E. Greer, "CORONA," *Studies in Intelligence*, Spring 1973; reprinted in *CORONA: America's First Satellite Program*, Kevin C. Ruffner, ed. (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 1995), p. 37.

[21] Greer, "CORONA," p. 1.

> sure that the secrecy stamp is absolutely appropriate before sealing up an operation inside the security cocoon.[22]

Mr. J.S. Gordon, the current President of Lockheed Martin Skunk Works, elaborated further on some of industry's concerns about secrecy policy:

- In original classification, the government has often relied on outdated perceptions concerning the value of the information, the whims of an overzealous classification official or, if all else fails, the status quo.
- Overclassifying technology inhibits information exchange between programs and leads to "reinventing the wheel."
- Classifying contractual and financial data within a corporation, which in today's environment should rarely be classified, inhibits accurate forecasting, limits oversight, and could eventually lead to an erosion in shareholder value based on unavailability of information for analysis.
- From a legal standpoint, classifying unnecessary paperwork can put the company and the customer in jeopardy of union actions and lawsuits.[23]

It appears, then, that official secrecy often exceeds the identifiable requirements of national security. If secrecy provides political "cover" and shields certain programs from the prying eyes of overseers, it also imposes an unwelcome burden on the "knowledge producers" themselves.

An Official Critique: the 1970 Defense Science Board Report

The disadvantages that secrecy imposes on knowledge production have not gone unnoticed by the government agencies that are the authors of that secrecy.

These disadvantages were described with unusual clarity by a 1970 Defense Science Board Task Force on Secrecy, created by the Director of Defense Research and Engineering and submitted to the Secretary of Defense. The Task Force, chaired by Dr. Frederick Seitz, concluded notably that "more might be gained than lost if our nation were to adopt—unilaterally, if necessary—a policy of complete openness in all areas of information."[24] Further:

---

[22] Ben R. Rich and Leo Janos*, Skunk Works* (Boston: Little, Brown & Company, 1994), pp. 333-34.

[23] J.S. Gordon, Point Paper, "Response to Commission on Protecting and Reducing Government Secrecy Request for Information," Lockheed Martin Skunk Works, 13 September 1995, available at <http://www.fas.org/sgp/othergov/skunkworks.html>.

[24] The Task Force quickly added, however, that "in spite of the great advantages that might accrue from such a policy, it is not a practical proposal at the present time." *Report of the Defense Science*

> With respect to technical information, it is understandable that our society would turn to secrecy in an attempt to optimize the advantage to national security that may be gained from new discoveries or innovations associated with science and engineering.
>
> However, it must be recognized, first, that certain kinds of technical information are easily discovered independently, or regenerated, once a reasonably sophisticated group decides it is worthwhile to do so. In spite of very elaborate and costly measures taken independently by the US and the USSR to preserve technical secrecy, neither the United Kingdom nor China was long delayed in developing hydrogen weapons.
>
> Also, classification of technical information impedes its flow within our own system, and may easily do far more harm than good by stifling critical discussion and review or by engendering frustration. There are many cases in which the declassification of technical information within our system probably had a beneficial effect and its classification has had a deleterious one:
>
> (1) The U.S. lead in microwave electronics and in computer technology was uniformly and greatly raised after the decision in 1946 to release the results of wartime research in these fields.
>
> (2) Research and development on the peaceful uses of nuclear reactors accelerated remarkably within our country, as well as internationally, once a decision was made in the mid-1950s to declassify the field.
>
> (3) It is highly questionable whether transistor technology would have developed as successfully as it has in the past 20 years had it not been the object of essentially open research.[25]

The Task Force also offered the following "sociological" observation:

> it was noted that the laboratories in which highly classified work is carried out have been encountering more and more difficulty in recruiting the most brilliant and technical minds. One member of the Task Force made the pessimistic prediction that, if present trends continue for another decade, our national effort in weapons research will become little better than mediocre.[26]

As if to confirm this latter prediction, U.S. Army General (ret.) William E. Odom wrote recently that most military laboratories have become worse than useless:

> Major savings could be achieved by abolishing virtually all the Defense Department and military service laboratories. Few of them have invented anything of note

---

Board Task Force on Secrecy, Office of the Director of Defense Research and Engineering, 1 July 1970. <http://www.fas.org/sgp/othergov/dsbrep.html>.

[25] *Report of the Defense Science Board Task Force on Secrecy*, p. 9.

[26] *Report of the Defense Science Board Task Force on Secrecy*, p. 11.

> in several decades, and many of the things they are striving to develop are already available in the commercial sector . . . Because they are generally so far behind the leading edges in some areas, they cause more than duplication; they also induce retardation and sustain obsolescence.[27]

Conclusion

There is a remarkable consensus among all concerned that secrecy has an adverse effect on the production of technical knowledge. At a minimum, secrecy increases costs and diverts precious resources into the large security infrastructure.[28] At a maximum, secrecy produces intellectual stultification and shields corruption or mismanagement.

Against this view, it can be argued that secrecy is nevertheless sometimes necessary to protect a sensitive technology from adversaries who would seek to duplicate it or negate its value. Though not strictly a legitimate function, secrecy can also protect a fragile program from domestic political interference or opposition.

There is a further consensus among all concerned that there is "too much" secrecy. It would be difficult or impossible to find any official spokesman who would claim that official secrecy is already at its essential minimum level and must not be reduced further. Unfortunately, however, this consensus exists only on a general plane. As soon as the secrecy of a particular program or category of information is called into question, the consensus breaks down. Many a classified program manager will doubt the need for secrecy in someone else's program, but is certain that his own program must remain secret.

As a result, it has proved difficult to substantially reduce the scope of official secrecy in technology, although some notable steps have been accomplished in the last several years by the Department of Energy, the Air Force and other agencies, due to agency leadership at senior levels.

---

[27] Lt. Gen. (ret.) William E. Odom, *America's Military Revolution: Strategy and Structure After the Cold War* (Washington, DC: The American University Press, 1993), p. 159. For a more nuanced appraisal of the problems of a particular laboratory, including its "culture of insularity," see Commission on Physical Sciences, Mathematics, and Applications, National Research Council, *1997 Assessment of the Army Research Laboratory* (Washington, DC: National Academy Press, 1998).

[28] The total classification-related security costs in government and industry reached $5.2 billion in FY 1996, according to the Information Security Oversight Office "1996 Report." This includes the costs of information security, physical security, and personnel security. Some three million citizens hold security clearances for access to classified information, which must be periodically reviewed.

But if it is true that secrecy is incompatible with knowledge production, this may turn out to be a self-correcting problem over the long term. To the extent that secrecy fosters inefficiency and stifles creativity, innovation will increasingly be found outside of the secret laboratories, which may eventually suffocate in their own splendid isolation.

Appendix A

SECRET

THIS DOCUMENT CONSISTS OF 1 PAGE
NO. 1 OF 2 SERIES

UNITED STATES
ATOMIC ENERGY COMMISSION
WASHINGTON 25, D. C.

* 19940000081 *
DOE-OR

4234

April 17, 1947

U. S. Atomic Energy Commission
P. O. Box E
Oak Ridge, Tennessee

Attention: Dr. Fidler

Subject: MEDICAL EXPERIMENTS ON HUMANS

1. It is desired that no document be released which refers to experiments with humans and might have adverse effect on public opinion or result in legal suits. Documents covering such work field should be classified "secret". Further work in this field in the future has been prohibited by the General Manager. It is understood that three documents in this field have been submitted for declassification and are now classified "restricted". It is desired that these documents be reclassified "secret" and that a check be made to insure that no distribution has inadvertantly been made to the Department of Commerce, or other off-Project personnel or agencies.

2. These instructions do not pertain to documents regarding clinical or therapeutic uses of radioisotopes and similar materials beneficial to human disorders and diseases.

ATOMIC ENERGY COMMISSION

O. G. HAYWOOD, JR.
Colonel, Corps of Engineers.

RESTRICTED DATA

CLASSIFICATION CANCELLED
AUTHORITY: DOE/SA-20
BY H.R. SCHMIDT, DATE:
HRSchmidt 2/22/94

SECRET