Post–Cold War Secrecy Policy

Greg S. Elkmann

Program on Information Resources Policy

Harvard University

Center for Information Policy Research

Cambridge, Massachusetts

A publication of the Program on Information Resources Policy.

Post–Cold War Secrecy Policy

Greg S. Elkmann
June 1994, P-94-1

Greg S. Elkmann wrote this paper as a Visiting Fellow from the National Security Agency.

ISBN 1-879716-07-0

Printing 5 4 3 2 1

June 1994

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

American Telephone & Telegraph Co.
Apple Computer, Inc.
Applied Telecommunications Technologies, Inc.
Arthur D. Little, Inc.
Australian & Overseas Telecommunications Corp.
BellSouth Corporation
Braxton Associates
Commission of the European Communities
Computer & Communications Industry Assoc.
DACOM (Korea)
Deloitte & Touche
Dialog Information Services, Inc.
DRI/McGraw Hill
Educational Testing Service
EG&G Inc.
ESL Inc.—a TRW company
ETRI (Korea)
European Parliament
France Telecom
Gartner Group, Inc.
GTE Corporation
Hitachi Research Institute (Japan)
IBM Corp.
International Data Corp.
International Resource Development, Inc.
International Telecommunications Satellite Organization (INTELSAT)
Korea Telecom
Lee Enterprises, Inc.
Lincoln Laboratory, MIT
Martin Marietta Corp.
John and Mary R. Markle Foundation
McCaw Cellular Communications, Inc.
MeesPierson (U.K.)
Mead Data Central
MITRE Corp.
National Telephone Cooperative Assoc.
The New York Times Co.
NEC Corp. (Japan)
Nippon Telegraph & Telephone Corp. (Japan)
North Communications
Northern Telecom
NYNEX
Pacific Bell
Pacific Bell Directory
Pacific Telesis Group
Puerto Rico Telephone Co.
Research Institute of Telecommunications and Economics (Japan)
Revista Nacional de Telematica (Brazil)
Samara Associates
Scaife Family Charitable Trusts
Siemens Corp.
Southam Inc. (Canada)
Southern California Edison Co.
Southern New England Telecommunications Corp.
Sprint Communications Company L.P.
State of California Public Utilities Commission
Strategy Assistance Services
The College Board
Thomson Professional Publishing
Times Mirror Co.
United States Government:
- Department of Commerce
  - National Telecommunications and Information Administration
- Department of Defense
  - National Defense University
- Department of Health and Human Services
  - National Library of Medicine
- Federal Communications Commission
- National Security Agency
- U.S. General Accounting Office

U.S. Media Group
Viacom Broadcasting
VideoSoft Solutions, Inc.
VISA International

Acknowledgements

The author gratefully acknowledges the following people who either provided information and helpful suggestions or who reviewed and commented critically on the draft version of this report:

Steven Aftergood
Clint C. Brooks
Fred R. Demech
James J. Fitzgibbon
Ronnie L. Goldberg
Morton Halperin
Roger Heusser
Jonathan A. Huneke
George F. Jelen
Robert Johnson
M.J. Levin
Fred Mannke
Lionel H. Olmer
L. Britt Snider
Charles J. Tringali

The author also thanks the National Security Program, John F. Kennedy School of Government at Harvard University.

They and the Program's affiliates, however, are not responsible for or necessarily in agreement with the views expressed here, nor are they to be blamed for any errors of fact or interpretation.

Executive Summary

The end of the Cold War provides an opportunity to reexamine many fundamental U.S. security assumptions, such as government secrecy. Since World War II, national security secrecy, driven by the wide ranging nature of the Cold War and by evolving technological trends, required the regulation of previously non-national security government and commercial information and technology. Although during the Cold War an expansive secrecy system may have been essential, it had serious impacts on other U.S. priorities, such as economic competitiveness and civil liberties, that need to be re-examined in light of the new world situation.

Prior to the late 1940s, secrecy was limited to obvious military targets, such as cryptography, weapon systems, military plans, or foreign policy decisions. That scope was narrow enough so that secrecy had little or no effect on the daily lives of the average person. Starting with the formation of COCOM in 1948 and the introduction of an expansive classification system by President Truman in 1950, secrecy restrictions began to intrude into many elements of everyday life.

Although the end of the Cold War has brought a visible reduction in secrecy, changing missions and technology advancement are still used to justify the introduction of new mechanisms, for example, the Clipper chip, giving an appearance of increased secrecy at a time when many believe secrecy can be reduced.

Discussions of government secrecy have often been limited to the military classification system, but the government uses many other techniques to restrict dissemination of information and technology. This report explores secrecy as it evolved in the Cold War, treating any government action that limits, delays, or prevents dissemination of information or technology for national security reasons as an element of secrecy policy. In 1993, the scope of secrecy policy was still widespread and included areas such as classification, export control, technology transfer, limitations on unclassified military technology, foreign investment, scientific communication, and civil liberty questions such as prior restraint on the media, limitations on topics the media can cover, executive privilege, and restrictions on government employees.

The effectiveness of U.S. secrecy policy involves both the strength of each element and also the interrelationships of elements. Modifications of the secrecy policy in one area often has repercussions in the secrecy of related elements, either requiring changes in order to remain consistent with overall policy or developing potentially damaging holes in the overall policy. For example, changing export control regulations may affect foreign investment decisions or changing the classification system will influence the scope of prior restraint on the media. This report looks at the assumptions and tradeoffs of major elements of the secrecy policy individually as well as through their interrelationships.

Because of the close correlation among those elements, many important issues and tensions recur in a number of areas. Although some unique issues surface in each secrecy element, the decisionmaker continually faces the same basic security, economic, and civil liberty tradeoffs. For example, increasing the priority of economic competitiveness requires

fewer export controls, less restriction on technology development, and more open investment. Understanding the relationships among these tradeoffs clarifies the effects of decisions as well as promotes consistent decisions.

One reason the same unresolvable tensions recur is because they do not lend themselves to obvious compromises. These tensions usually occur in the following situations:

- picking the proper secrecy objectives;
- establishing the proper scope of the secrecy controls;
- balancing national security benefits against economic costs;
- balancing national security benefits against social costs; and
- conforming with political realities.

This report explores a number of the tensions that influence the direction of U.S. security policy. A fundamental problem of secrecy is that it must reflect reality, not the desires of the national security community. Economic, social, and technologic trends must be factored into the policy. The integrated world economy and exploding technology development vastly reduce the amount and type of information and technology that the U.S. can control, even though national security may call for greater secrecy. For example, export controls have to deal with the fact that almost all critical U.S. technology can bought from other countries and that only international cooperation can prevent further dissemination. Socially, the U.S. public is demanding more information and greater accountability from the government, even when these demands run counter to perceived national security, as in the debate over public cryptography, where the government's understandable reluctance to provide detailed explanations of its cryptographic standards are viewed very skeptically by the public.

A second fundamental tension is the way in which the government implements secrecy. The U.S. was founded on the principle of democracy fueled by informed public debate. Most government institutions need openness to perform effectively, although some require secrecy. Conflicting missions, as when the Department of Commerce promotes international sales while the Department of Defense pushes for greater export control, have brought about emergence of a hodgepodge of secrecy regulations without a coherent philosophy. Even the "same" secrecy policies are implemented differently by various departments, each reflecting its own priorities.

Contents

Illustrations

Figures

Tables

Chapter One

Secrecy and Its Uses

> Without clearly defining what we mean by national security, we have turned it into a talisman to ward off any evil that might befall us as a nation.
>
> John Shattuck[1]

1.1 Introduction

"Protect all the information that needs protecting and nothing more" is a cliché that has been integral to the United States' national security secrecy system throughout the Cold War. Although this attitude may sound like a common sense approach to balancing the requirements of national security with other democratic imperatives, its implementation has proved difficult and contentious. Few people disagree with the premise that some information and technology need to be protected from disclosure, yet many others, ranging from industry leaders to congressional representatives to civil libertarians, think that much unnecessary information has been subsumed into the secrecy system and that restrictions imposed by secrecy have been too stringent. Such critics believe secrecy achieved its objectives but only by damaging other national goals. Tension about the proper role of secrecy arises from questions about the government's basic secrecy policy—which information needs to be protected and the degree of protection necessary—that are inherently subjective and depend on the evolving national security consensus. In an attempt to find a suitable balance nearly every U.S. president during the Cold War modified the parameters between secrecy and openness in relation to ideology, the perceived current military situation, congressional mandate, and internal political pressures.

Even with the end of the Cold War, national security remains a powerful driving force in the U.S. The comforting assumption, maintained throughout that era, that "national security" could be defined precisely is fading fast. For the last forty-five years, it meant that the U.S. had to be prepared to stop a direct military attack from the (former) Soviet Union or its surrogates. National security objectives consisted of strengthening the U.S. and its allies and weakening the Soviet Union and its allies, or at least delaying attempts by the Soviet Union to strengthen itself. Those objectives are no longer sufficient. In the evolution of a post-Cold

War national security strategy, many other concerns—such as regional stability or counter-terrorism—are becoming more central and their contributions to the national interest more recognized.

During the Cold War information policy was an integral part of the national security strategy. For example, the U.S. policy of delaying improvement of the Soviet military hinged on reduction of its military and industrial capacity through denying it access to the latest technology by placing secrecy restrictions on information and technology. The restrictions included classification of information and military technology, setting export controls on military and dual-use[2] technology, restricting scientific communication and research, and restricting the operation and ownership of defense firms.

As the post-Cold War situation emerges it will require a new national security strategy adapted to meet changing military requirements and threats. Cold War strategies and tactics, although successful in opposing the Soviet Union, must give way to new ones. Some form of secrecy restrictions will continue to be part of the policy, but the end of the Cold War gives the U.S. the opportunity to reexamine cost and benefit tradeoffs in current policy and to decide on the best policy to meeting evolving concerns.

1.2 National Security Restrictions

Secrecy restrictions in this report include more than the formal government classification system, introduced in 1982 by President Reagan,[3] which controls only information or technology that, if released, might cause the U.S. damage. Other restrictions controlled unclassified information and technology that were necessary to protect from the Soviet Union, including:

- Redefinition of the classification system to increase its scope
- Export control
- Restrictions on publication of dual use scientific literature
- Limitations on attendance by foreigners at scientific conferences on dual-use technology
- Control of media coverage of certain military engagements
- Prepublication approval required of all former government officials

- Secret patents
- Restrictions on the foreign ownership of defense firms
- Restrictions on conversion of military technology to the commercial sector
- Restrictions on commercial research and development (R&D) in militarily sensitive technologies
- Restrictions on the commercial capabilities of militarily sensitive technology

Although the effectiveness of individual restrictions is difficult to gauge, history suggests that the effect of all of them taken together were fairly successful in achieving their objectives, such as delaying Soviet acquisition of important military technology or delaying countermeasure against U.S. weapons systems. Yet secrecy restrictions also had significant costs for the U.S., direct and indirect, such as interference with advancement of commercial technology and decreasing the competitiveness of the U.S. economy through export controls. When the appropriate levels of secrecy are determined for the new national security strategy, the costs and benefits of these restrictions will need to be balanced.

1.3 National Security Mindset

Security was not the result of implementation of a few scattered protection mechanisms but an integral part of the government security strategy that required government control of areas previously unregulated, such as commercial technology development. In the battles of the Cold War, national security demanded more than military power—although it required military preparedness—it depended on such concepts as the development and maintenance of a technological advantage in military and commercial technology, a national resolve to use the military to stop the spread of communism, regulation of U.S. international trade, and patience to continue the Cold War struggles indefinitely. The increased scope of national security requirements brought about a mindset according to which national security was given the highest societal priority and every other issue became secondary. Neither developed by government to increase its own power nor imposed on an unwilling public, this mindset was largely the consensus of the people and their government. John Shattuck, currently Assistant Secretary of State for Democracy, Human Rights, and Labor under President Clinton, offered a good description of the beginning of this mindset:

> What is most remarkable about all of this is that we seem to have drifted into a state of permanent emergency that has no immediate context. We do not know what the emergency is or how long it will last. We do not even have a

> clear understanding of its impact on our system of liberty since we have been conditioned to accept the view that the rule of law often requires individual liberties to yield to claims of national security under certain limited conditions.[4]

In the public debate major issues were framed in relation to their effect on the balance between the U.S. and the Soviet Union, even in the absence of obvious connection between that balance and the issues. Advocates of policies perceived as hostile to national security—for example, advocates of liberal export control policies and of freedom of the press—needed to show that reducing restrictions would not cause harm to the U.S. Policies that resulted in slightly higher military risk but that also achieved substantial gains in other sectors, such as economic growth, were met with suspicion. A statement by Senator Henry Jackson in 1980 illustrates how the national security mindset gave more weight to national security arguments; complaining that proponents of liberalized international trade, supposedly an inherent civil liberty, had suggested that the legislation he was discussing should be adopted unless the government could show direct national security damage, Jackson said: "The burden of proof has been placed on those seeking to protect our national security. . . . Our export control system has been turned upside down."[5]

Foreign policy and military action often were responses to Soviet intentions and threats. The Bay of Pigs, Korea, Vietnam, the Cuban missile crisis, Nicaragua, Afghanistan, and many other foreign policy decisions during the Cold War were based on deterring communist aggression, regardless of any effect on other national interests. Owing to such concerns, the cause of national security led the government to violate U.S. law. Civil liberties were sometimes compromised by successive administrations lying to the public, illegal spying by intelligence agencies, and limitations on the freedom of the press. Even in the 1990s, with the Cold War ended, public debate on most issues is still framed in terms of national security.

Secrecy is closely linked to the national security mindset. The secrecy system helped develop the mindset, and a natural outgrowth of increased security awareness is reliance on more secrecy. Secrecy encouraged this mindset by inspiring public fear of the Soviet Union, for example, by keeping hidden details of the real Soviet threats and intentions. A fearful and uninformed public were more likely to believe the worst about the Soviet Union and demand increased national security measures. Almost any information could help the Soviet Union in

some way, but protecting it all was impractical. Decisions had to be made about what to protect, and how; because insufficiently protecting information meant helping the Soviets, the natural reaction was to be conservative and restrict any information that did not need to be released. The cycle of secrecy became self-reinforcing: the less the country knew of the true magnitude of the Soviet threat, the more concerned the country became, increasing the importance of national security and leading finally to greater secrecy to protect national security information.

One outcome of reinforcement was degradation of public debate on national security issues, which continues today. During such a debate, the government can discuss only selected, unclassified portions of an issue, while critics may discuss any aspect they choose. Often, through ignorance or advocacy, the critics introduce incorrect information. The government, although aware the information given to the public is false, cannot respond to incorrect arguments, because to answer them would require revealing classified information. Thus, even national security issues that enter in public debate can sometimes be argued from incorrect premises.

Steven Katz, of the American Civil Liberties Union (ACLU), sums up the consequences of the national security mindset very well:

> The criteria for restricting access is generally summarized under the concept of national security. But "national security," like "foreign policy," is as much a point of view as it is a discernible set of principles. When "national security" is invoked, it is a formidable justification to overcome by those fighting to resolve the conflict between civil liberties and ideology, preserve the role and responsibility of the press, ensure the free flow of information, and affirm the people's "right to know" in a democratic society.[6]

Yet a note of caution must be sounded about the extent of the national security mindset. By the standards of the world and even of other democratic countries, the U.S. is not a closed society. Commenting on defense information, Gordon Adams of the Defense Budget Project said:

> What is striking about the role of elected legislators in the defense budget is the staggering volume of information they receive on the budget. Observers from other countries are often overwhelmed by the amount of information published by the administration on the defense budget . . . . Despite the suspicion that may exist between the military and Congress, by contrast with

> the military of virtually any other country in the world the Pentagon is a veritable fount of information. From the start, Congress faces less of a problem ferreting out secrets from the Pentagon than it does shifting through the volume of data to separate the important from the insignificant.[7]

The British Official Secrets Act (1989),[8] which forbids unauthorized release of any government information, provides an example of how laws in other democratic countries treat information. The comparable U.S. law, the Freedom of Information Act (FOIA) mandates the release of most government information.

1.4 Secrecy Policy

The proper role of information policy, including secrecy, should be determined by the evolving balance between U.S. national security interests, its economic interests, and democratic rights of freedom of the press and access to public information. The policy choices that advance one set of interests often have negative impacts on others.[9] Since the beginning of the Cold War, national security has been the primary U.S. priority, and conflicts among policy choices have usually favored its priority. The disintegration of the former Soviet Union has drastically changed the global political, economic, and military environment. The perceived threat to the U.S. has changed from direct military confrontation with the Soviets to confronting regional instability and global economic challenges.

Government and commercial secrecy as important strategy for the handling of information and technology was ingrained during the Cold War. The U.S. strategy then was to compensate for the large size of Soviet conventional forces by developing a high-technology military. Secrecy delayed Soviet access to technology with military applications at the same time that it protected conventional military information. Many critics think excessive secrecy had a significant cost, especially for the U.S. economy. They think government secrecy adversely impacted the commercial economy by monopolizing and slowing technology transfer to the commercial sector, which caused U.S. corporations to lose marketshare through export control and slowed public research that overlapped military technology, and allowing industries to become noncompetitive. Secrecy also adversely impacted the kind and amount of information available to the public. In 1970 in a report on the classification system, the Defense Science Board stated:

> On the negative side, in addition to the dollar costs of operating under conditions of classification and of maintaining our information security system, classification establishes barriers between nations, creates areas of uncertainty in the public mind on policy issues, and impeded the flow of useful information within our country as well as abroad.[10]

Government strategy will always require secrecy as one element, but the scope of what needs to be kept secret changes in response to the dynamics of national security and economic competitiveness.

1.5 Policy Considerations

The task of developing an appropriate policy of secrecy is difficult. A number of considerations need to be interwoven to develop a policy that will best meet the criteria of effectiveness, minimal cost, and preservation of the balance between security and other priorities.

The first consideration is to determine which national interests are supported by a secrecy policy. During the Cold War, the national interest was clear and remained stable for long periods. The definition—anything that helped the Soviets damaged U.S. national security—was independent of the particular world situation. While that definition was vague enough to lead to disagreement on many details, the theme was known and a consensus emerged. With the passing of the Soviet Union, no such consensus guides policy. The world situation is so unstable that U.S. national security is decided on a case-by-case basis. Policy has become reactive, instead of providing a road map for future decisions. Even though no stable, explicit definition of national security may be possible, general principles remain necessary when making tradeoffs for an updated secrecy policy. Because such principles are still evolving, this paper uses the national objectives described by former President Bush, who adopted the following U.S. interests and objectives for the 1990s:

- The survival of the United States as a free and independent nation, with its fundamental values intact and its institutions and people secure.

- A healthy and growing U.S. economy to ensure opportunity for individual prosperity and resources for national endeavors at home and abroad.

- Healthy, cooperative and politically vigorous relations with allies and friendly nations.

> • A stable and secure world, where political and economic freedom, human rights and democratic institutions flourish.[11]

Recent (1989) opinion polls[12] found that the public regards economic competitiveness as the biggest component of the national interest, even higher than national security.

National security, although vitally important, is only one of many democratic rights to be considered. In a democratic society, the public has a fundamental "right to know." It needs enough information, provided in a timely fashion, to participate in informed debate. In the name of national security, secrecy places limitations on dissemination of the information needed by the public and has resulted in uninformed and manipulated debates on some crucial issues. The best example is the entry of the U.S. into war in Vietnam. As the Pentagon papers detailed, relevant information that might have changed the historical outcome, was not revealed.[13] In general, the government, through selective declassification and leaks, directed public debate on Vietnam in ways that supported its policy. Secrecy can also shield government failures from entering public debate, as shown in the current, if muted, debate on the U.S. over arming Iraq before Desert Storm. Future secrecy policy should take into account government's tendency to manipulate public information.

Another democratic right is public accountability. For democracy to function, the public has to trust the government. One important part of developing such trust is the accountability of the government. The people have a "right to know" what activities the government is engaging in, what its rationale is for its actions, and when its activities are taking place. The promotion of accountability was a driving force behind the Freedom of Information Act (1973 Amendment).[14] Obviously, secrecy is a deterrent to accountability. An appropriate balance needs to be struck.

Economic competitiveness is considered a priority separate from but not necessarily subordinate to national security. During the Cold War, U.S. national economic policy was subordinated to national security policy in several important areas. Such issues as international export, foreign ownership of U.S. companies, R&D, and limits to commercial technology all were more national security, rather than economic, decisions. Mickey Kantor enunciated this view in testimony before the Senate at the time of his nomination as U.S. Trade Representative:

> What we need to look at. . .is creating economic viability at home. If we do that, that is part of our national security. . . . Our economic viability is critical if we're going to exercise the kind of influence we want to exercise in this very dangerous world that we face.[15]

Economic issues need to be decided on their own merits, while also supporting national security objectives.

To determine appropriate policy, a number of characteristics of each secrecy restriction or mechanism must be analyzed. Each restriction is intended to achieve different objectives, has different costs, different effectiveness, and interacts differently with the other restrictions. Each restriction can be analyzed separately to assess its strengths and weaknesses, then the collection of restrictions can be analyzed together to assess strengths and weaknesses of the policies to achieve the set of restrictions that best meet the objectives at the lowest overall cost. Because the world changes, tradeoffs will never be stable but will constantly evolve, and U.S. policy should be flexible enough to adapt to changes.

An analysis of the secrecy restrictions requires determining the goals that secrecy policy supports. The overall policy comprises smaller policy objectives; no single secrecy restriction or set of restrictions will meet the entire secrecy policy, but each restriction will help to achieve a subset of it and together all of them should achieve the entire policy objectives.

Analysis of secrecy restrictions yields characteristics important for determining their effectiveness and practicality, including specific policy objectives each restriction supports, the scope of these objectives relative to the entire policy, how well each meets its policy objective, how necessary each is for meeting that objective, and the interrelationships among the various restrictions which affect their effectiveness. The secrecy costs can be direct economic costs—the resources used in running the system or the lost sales—or indirect economic and social costs—reduction in development of technology or in civil liberties. The secrecy policy in use at any given time consists of the set of restrictions that best balance effectiveness and total costs while still meeting the national objectives.

1.6 A New Light on Secrecy

This paper examines secrecy policy from the perspective of the new international situation, focusing primarily on the changing tradeoffs between the costs and benefits of the restrictions of the Cold War and applied to national security objectives in the wake of that era. Secrecy here is treated as any government restriction on information or technology used to fulfil a national security objective. This definition is extremely broad and encompasses many topics, from classification to export control to commercial technology restrictions, topics not ordinarily associated with secrecy. On the other hand, espionage, traditionally part of secrecy, is not discussed here, because it is not affected by changes in the government's information policy. Owing to this expansive scope, the paper is limited to a brief overview of the U.S. secrecy system and discussion of broad policy questions.

Three main ideas are addressed here. First, the background of the Cold War secrecy system is discussed, a short overview of its history in **Chapter Two** and the secrecy mechanisms themselves, how they were applied during the Cold War, and their effects in **Chapter Three**. Second, particular secrecy mechanisms now in use, including the present formal classification system, technology transfer (e.g., limitations on commercial technology), limitations on Foreign Direct Investment (FDI) of defense firms, export control, defense conversion, and civil liberties limitations are examined in **Chapters Four** through **Eight**. Each chapter looks at a mechanism from the perspective of benefits, costs, and major policy questions and tradeoffs for the post-Cold War period. Last, The focus of the paper shifts in **Chapter Nine** to the secrecy policy as a whole. Many of the broad policy issues that influence several different restrictions need to be addressed comprehensively. This chapter identifies and examines the meaning of these issues and tradeoffs to overall secrecy policy in the post-Cold War period.

Notes

1. U.S. Congress. House Committee on the Judiciary. John Shattuck, Testimony before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice. *1984: Civil Liberties and the National Security State*. 98th Cong., 1st and 2d sess., 1983-1984, Committee Print 103, p. 337; hereafter referred to as *1984: Civil Liberties*.

2. Dual-use technology is technology that has commercial and military application, including such products as computers and airplanes and technology such as improved manufacturing processes.

3. Executive Order 12356, 47 Federal Registry 14874, April 6, 1982.

4. Shattuck, *1984: Civil Liberties*, 336.

5. U.S. Congress. Senate. Permanent Subcommittee on Investigations of the Committee on Governmental Affairs. *Transfer of Technology to the Soviet Bloc*. Opening statement of Senator Henry Jackson. 96th Cong., 2d sess., Feb 20, 1980, Committee Print, p. 5.

6. National Commission of Libraries and Information Science, *Hearing on Sensitive but not Classified Information*, Steven Katz, Opening Testimony, May 28 1987, p. 11.

7. Gordon Adams, *The Role of Defense Budgets in Civil-Military Relations* (Washington, D.C.: Defense Budget Project, 1992), 15-16.

8. Official Secrets Act of 1989, United Kingdom, May 11, 1989.

9. Proof that the U.S. policy was advantages was the fact that during the Cold War, the Soviet Union spent more in percentage of GNP devoted to national security than did the U.S.

10. Defense Science Board, "Report of the Defense Science Board Task Force on Secrecy," Office of the Director of Defense Research and Engineering, Washington, D.C., July 1, 1970, 1.

11. George Bush, *National Security Strategy of the United States* (Washington, D.C.: The White House, 1991), 3-4.

12. Daniel Yankelovich, "Foreign Policy After the Election," *Foreign Affairs* **71**, 4 (Fall 1992), 8; according to Yankelovich, citing an ABC News–*Washington Post* poll of February 1989: "Similarly when national security and economic interests collide people give priority to the economic side of policy, partly on the grounds noted earlier, that America's present economic weakness is seen as the larger threat to national security." Note that the poll was taken prior to the 1990 recession and the 1991 breakup of the Soviet Union.

13. Morton H. Halperin and Daniel N. Hoffman, *Top Secret: National Security and the Right to Know* (Washington, D.C.: New Republic Books, 1978), 8-11.

14. U.S. Congress. House. Subcommittee of the Committee on Government Operations. *The Freedom of Information Act*. 93 Cong., 1st sess., May 2, 1973. p. 1; hereafter Freedom of Information Act. In his opening statement, Congressman Moorehead stated that "In the first place, we are nowhere near the goal of a fully informed public in a democratic society which was the hope of those who started the freedom of information fight. In the second place, the freedom of information law did not become the weapon the free press needed to fight against secrecy."

15. U.S. Congress. Senate. Committee on Finance. *Confirmation Hearing for Mickey Kantor, United States Trade Representative-Designate*, Testimony of Mickey Kantor, 103 Cong., 1st sess., Jan. 19, 1993.

Chapter Two

History of Secrecy Regulations

> I do believe the question of secrecy in the executive branch remains in the last analysis one of applied commonsense on the one hand and of the felt pressures of a free-speaking democratic system on the other.
>
> William P. Bundy[1]

2.1 Early History

Given national security's central role in today's society, its extensive intrusion into ordinary life is surprisingly recent. The wide-ranging national security restrictions on information and technology were instituted primarily after World War II. Before then, secrecy had generally been limited to national security information directly concerned with military operations, weapons, military installations, or foreign policy. The legal authority to impose restrictions was limited to the departments of the Army and Navy. Since the 1940s, when national security ceased being strictly a function of military strength, it has grown into a larger concept that includes many areas with little direct connection to the military yet concerned with promotion of national interests of the United States.

That is not to say secrecy is entirely new. Since the beginning of the U.S., forms of secrecy have existed. The Housekeeping Statutes of 1787, which authorized the original cabinet departments, included wording that was used to justify withholding information from the American public. Although the information withheld was not formally classified as classification has come to be defined in the twentieth century, the statutes were the means by which nonmilitary departments, particularly the State Department, could restrict access to national security and foreign policy information.[2]

In the nineteenth century, secrecy was used only in wartime. During the War of 1812, the U.S. military used classification markings but abandoned them after the war. Secrecy was similarly limited during the Civil War. The military restricted individual pieces of information but did not institute a comprehensive system of official secrecy. Peacetime secrecy procedures started in 1869, when the War department forbade photographs of frontier forts. Prior to

World War I, secrecy was not a major public issue, and restrictions remained minimal until the war.[3] **Table 2-1** gives a chronology of secrecy restrictions.

Table 2-1

Classification History

Year	Event	President
1789	Housekeeping Statutes	
1917	Espionage Act	
1938	Enabling Legislation (52 Stat. 3)	
1940	E.O.* 8381 (based upon 1938 law)	Roosevelt
1946	Atomic Energy Act	
1947	National Security Act	
1950	E.O. 10104	Truman
1951	E.O. 10290	Truman
1952	Invention Secrecy Act	
1953	E.O. 10501	Eisenhower
1954	Atomic Energy Act amended	
1961	E.O. 10964	Kennedy
1972	E.O. 11652	Nixon
1978	E.O. 12605	Carter
1982	E.O. 12356	Reagan
1982	Intelligence Identity Act	
1984	NSDD 145	Reagan
1986	NTISSP No. 2	Reagan

*Executive Order.

During World War I, President Wilson introduced in the Espionage Act of 1917 the first legislation directed at establishing permanent secrecy restrictions. Its narrow definition of espionage should not be confused with the more modern definition of classified information. Significant amounts of material currently considered classified do not meet requirements for prosecution under that statute. Although amended several times to expand its definition of national defense, the statute has not changed much since enactment. To be prosecuted for

espionage, a person must acquire national defense information or technology with the intent or with reason to believe that it is to be used to the injury of the U.S. or to the advantage of a foreign nation.[4] Although the provisions of the act do not constitute a government classification scheme, the act provides a sense of the scope of national defense (security) information during World War I. It defines national defense information as information concerning any vessel, work of defense, military installation (including navy yard, fort, railroad, or wireless station), place where munitions and other material are made, stored, or repaired, or other places the president has determined would be prejudicial to the national defense; it defines information as a document, writing, code book, signal book, sketch, photograph, map, model, or instrument.[5] The intelligence community has interpreted the inclusion of code books as providing the authority to protect cryptographic information above and beyond the formal classification system. Rules granting the intelligence community greater protection occur also in many other regulations. The real effect of the Espionage Act, although unrelated to secrecy, was through its broad provisions for the suppression of public criticism of the government. During World War I, more than two thousand people were charged with espionage for criticizing or opposing the war.[6]

World War I saw the first systematic use by the military of classification markings. Adopted in November 1917, the U.S. classification system consisted of the "Secret, Confidential, and for Official Circulation Only" classifications used in the French and British systems.[7] Throughout the 1920s and '30s, classification continued to be limited to military and national defense information. The applicable Army and Navy department regulations defined a three-level classification system: Secret, Confidential, and Restricted. *Secret* was defined as information whose unauthorized release might endanger the national security, *Confidential* as information that might be prejudicial to the interests or the prestige of the U.S., and *Restricted* as information that should be limited for reasons of administrative privacy.[8]

In 1938, Congress again dealt with the question of protecting military information. Fundamental attitudes toward security had not changed, and the 1938 law closely followed the view of national security outlined in the Espionage Act of 1917. The new law allowed the president to designate, in the interests of national defense, vital military and naval installations or equipment as requiring protection against general dissemination. It outlawed unauthorized

photographs, sketches, pictures, drawings, maps, or graphical representations of such designated installations or equipment.

President Franklin Roosevelt invoked the 1938 law in March 1940 as the basis for the executive order (E.O. 8381) that instituted a government classification system.[9] Some historians claim Roosevelt exceeded his authority in issuing this order, because the 1938 law already authorized a classification system,[10] but the system that resulted was used during World War II to protect war-related information. The executive order continued the pre-war concept of a three-level classification scheme of Secret, Confidential, and Restricted but did not provide a concrete definition of what constituted correct classification under its provisions. E.O. 8031 defined vital military and naval installations or equipment subject to the provisions of the 1938 law as:

> (*i*) Previously classified (and anything classified in the future) installations and equipment located within:
>
> - Military or naval reservation
> - Defensive sea area
> - Airspace reservation
> - Naval harbor closed to foreign vessels
> - Areas required for fleet purposes
> - Commercial establishments engaged in development of military equipment
>
> (*ii*) Military aircraft, weapons, ammunition, vehicles, ships, vessels, instruments, and other military equipment
>
> (*iii*) Military books, pamphlets, documents and other written information.[11]

National security was still limited to military information and technology. Everything classified was directly connected with the dissemination of information about military targets. The major effect of the executive order was to consolidate the classifications systems being used by the Army and Navy. Although the order did not modify previous military definitions of classified military information, the authority to classify remained limited to the Secretary of War, the Secretary of the Navy, and their delegates.

2.2 Cold War Secrecy

In 1946, Congress began build-up of the Cold War secrecy system with the passage of the Atomic Energy Act (AEA). **Table 2-2** lists laws that affect secrecy.[12] The classification of Restricted Data in the AEA (different from the Restricted classification in E.O. 8031) and the concept of "born secret" were developed for nuclear information. All such information was now automatically classified as Restricted, which prohibited its release whether it was developed by government or private initiative. This act introduced the precedent that the government might regulate private information, thereby denying creators the fruits of their labors. Nuclear information differs from other information in that it does not need to meet a classification test before being protected. In 1954 the AEA was amended to allow declassification of selected nuclear information and to allow it to be shared with the commercial nuclear industry. The distinction of nuclear information as "born secret" was retained in 1954 and remains in effect today.

In 1947, Congress passed the National Security Act, which established the Central Intelligence Agency (CIA) and gave it responsibility for protecting intelligence information, including sources and methods, from unauthorized disclosure. The provisions of the Act have been interpreted as giving the CIA authority to protect intelligence information beyond that provided by the classification system, and it has been the basis for the security measures used by the intelligence community.[13]

The Cold War changed the parameters of war and the scope of national security information. For example, during World War II the national security objective was fairly simple: military victory on the battlefield. Other factors, ranging from technological advancement to industrial capacity to economic strength to public resolve, were concerns only to the degree they helped win battles. In the Cold War, the battle changed from direct military confrontation, which needed to be avoided because of the threat of nuclear war, to national potential, in which those other factors became battlefields unto themselves. This new paradigm shifted the scope of national security from military and foreign policy information to potentially everything in society. In the 1940s, it was not known what aspects of the military, the economy, or society contributed to eventual military power and therefore needed protection. In the early years of the Cold War period the government took a very conservative approach to secrecy. Society did not know what might be useful to the Soviets, so it protected

Table 2-2

Secrecy Laws

Laws	Public Law*	Statute
1. Espionage Act of 1917	Ch. 30	40 Stat 218
2. Trading with the Enemy Act of 1917	Ch. 106	0 Stat 411
3. Federal Communications Act of 1934	Ch. 652	8 Stat 1064
4. 1938 Act on Defense Secrecy	Ch. 2	52 Stat 3
5. Atomic Energy Act of 1946	Ch. 724	60 Stat 766
6. National Security Act of 1947	Ch. 343	61 Stat 495
7. Export Control Act of 1949	Ch. 11	63 Stat 7
8. Invention Secrecy Act of 1951	Ch. 4	65 Stat 805
9. Mutual Security Act of 1951	Ch. 479	65 Stat 5373
10. Atomic Energy Act of 1954	Ch. 1073	68 Stat 919
11. Freedom of Information Act (1966)	PL 89-554	80 Stat 383
12. Arms Export Control Act (1968)	PL 90-269	82 Stat 1321
13. Export Control Act of 1969	PL 91-184	83 Stat 841
14. Privacy Act (1974)	PL 93-579	88 Stat 1896
15. International Investment and Trade Survey Act (1976)	PL 94-472	90 Stat 2059
16. International Emergency Economic Powers Act (1977)	PL 95-223	91 Stat 1626
17. Export Control Act of 1979	PL 96-72	93 Stat 503
18. Stevenson–Wylder Technology Transfer Innovation Act of 1980	PL 96-480	94 Stat 2311
19. Bayh–Dole Act (1980)	PL 96-517	94 Stat 3019
20. Intelligence Identity Act (1982)	PL 97-200	96 Stat 122
21. Land Remote-Sensing Commercialization Act of 1984	PL 98-365	98 Stat 451
22. Export Administration Act of 1985	PL 99-64	99 Stat 120
23. Federal Technology Transfer Act (1986)	PL 99-502	100 Stat 1785
24. Computer Security (1987)	PL 100-235	101 Stat 1724
25. Omnibus Trade and Competitiveness Act of 1988	PL 100-418	102 Stat 1107
26. Multilateral Export Control Enhancement Amendments Act (1988)	PL 100-418	102 Stat 1364
27. National Competition Technology Transfer Act of 1989	PL 101-189	103 Stat 1674

*Prior to 1952 Public Laws (PL) were identified as Chapters (Ch.).
Note: References are to original bills, not to subsequent amendments.

everything. The expanded definition of national security information reflected the uncertainty about the scope of national security.

President Truman responded to the altered world situation by promulgating two executive orders on classification. The first (E.O. 10104),[14] added a fourth level of classification, Top Secret.[15] The second (E.O. 10290),[16] which expanded the scope of national security, was the true beginning of the current secrecy system. It made two significant contributions to the previous secrecy philosophy: it expanded those authorized to classify information from only the military and foreign policy communities to include all executive agencies and eliminated explicit references to traditional security concerns that had justified the previous executive orders. These modifications effectively allowed any federal employee to classify any information release of which could be considered potentially damaging to the U.S. The transformation of secrecy from the shadowy back rooms of the military, where it did not intrude on society, into something that affected all of society had begun.

E.O. 10290 defined *Top Secret* as information unauthorized access to which could cause exceptionally grave damage to national security, *Secret* as information that needs extraordinary protection, *Confidential* as information that needs careful protection, and *Restricted* as information that requires protection.[17] With only minor changes, this definition remains in use today. In 1953, sustained criticism of the Truman order, especially for its ambiguous definition of classification and for allowing all federal agencies to classify information,[18] caused President Eisenhower to modify the classification system (E.O. 10501).[19] This executive order made three major changes in the Truman order: it reduced the scope of the system by limiting the federal agencies granted classification authority, eliminated the Restricted classification level (although the distinct category of Restricted is retained for nuclear information*), and tried to narrow the definition of the levels by reestablishing a link to national security as a reason for classification.

According to E.O. 10501, information was Top Secret if it could lead to a definite break in diplomatic relations, an armed attack, a war, the compromise of military or defense plans, intelligence operations, or scientific developments vital to national defense. Secret was defined

---

*The Restricted Data in the AEA remains unaffected by this order.

as information that could jeopardize international relations, endanger the effectiveness of a policy of vital importance to the national defense, or defense plans and scientific developments important to national defense.[20] Although these definitions still permitted individual discretion, they also provided an underpinning of military and foreign policy objectives.

Elimination of the Restricted classification level did not have so large an effect on reducing classified material as might have been imagined. Some Restricted material was declassified and released, but a large percentage of it was reclassified as Confidential and remained protected.[21]

President Kennedy introduced automatic declassification in Executive Order 10964,[22] which directed the division of classified information into four groups, each with different declassification rules. Group 1 contained foreign government, atomic energy, and intelligence information but no automatic requirements for downgrading to Group 4, routine classified information that had been downgraded one level every three years and declassified after twelve.

The Freedom of Information Act (FOIA) altered the dynamics of government control of information and secrecy in the late 1960s. By this Act Congress declared a clear public interest in the release of government information and mandated release of executive branch information on request, subject to a few specific exceptions. Because one exception was for classified information, as defined by the president, the FOIA did not directly affect the classification system. In 1974 an amendment[23] introduced "in camera" judicial review of classification decisions, a provision seldom, if ever, used.[24] The concept of information disclosure as a public good, not previously explicit, had to be incorporated into government information policies. The major effect of the FOIA on classification was to introduce mandatory declassification review of requested information. The government had to prove that information whose release was denied under the FOIA exemption was properly classified at the time of the decision. Since 1967, significant amounts of information that would not have been otherwise released have been declassified through mandatory reviews.

President Nixon continued Eisenhower's tightening classification requirements. Changes included reduction of the number of agencies with authority to classify, decreased the time necessary for automatic declassification, and formation of an oversight committee to monitor the classification system.[25] In the introduction to the executive order he justified modification of the system: "The interests of the U.S. and its citizens are best served by making information regarding the affairs of Government readily available to the public. This concept of an informed citizenry is reflected in the Freedom of Information Act and in the current public information policies of the executive branch."[26]

The major impact of this executive order was to limit classification authority to twenty-six departments and to the Executive Office, giving only thirteen departments Top Secret authority.[27] The number that had original classification authority went from sixty thousand to twenty thousand.[28] In 1973, Nixon also introduced a systematic review process in which archival records were reviewed for declassification. Between 1973 and 1980, it resulted in declassification of 370 million pages, although after 1980 the number declined rapidly.[29]

The Privacy Act of 1974 added another complication to the government information policy. Congress mandated the "secrecy" of some unclassified government information on the grounds of the public right of privacy. Personal information collected by the government was restricted to the use originally intended when the information was collected. The Privacy Act mandated that the government must safeguard personal information from unauthorized access, similar to the protection required for classified information.

President Carter also continued the tightening of classification rules. In 1978, his executive order (E.O. 12065) modified Nixon's by reducing the minimum requirement for classification from "damage" to "identifiable damage" to the national security, further reduced the number of agencies that had original classification authority, decreased the time for automatic declassification to take effect, provided additional guidance to classifiers by introducing a list of categories to which information to be classified had to belong, introduced a balance test for declassification, and required that when the true classification level was in dispute the lower level (including Unclassified) should be used.[30]

Definitions of Top Secret and Secret remained constant, but that of Confidential now required identifiable damage to the national security. In addition, the order introduced a second test into the classification decision: information had to belong to one of seven categories before it could be considered for classification, including military plans or weapons, foreign government information, foreign relations of the U.S., intelligence sources and methods, and scientific, technological, or economic matters relating to national security. A catch-all category of "other relevant information" also was included,[31] defeating the purpose of the categories. Although the definitions remained ambiguous and most information could be shoehorned into the categories, the requirement of identifiable damage provided a much stricter test than had earlier executive orders on secrecy.

In the potentially most far-reaching change since Truman's original expansion of the classification system, Carter instituted an explicit requirement to balance public interest in disclosure against damage to national security during *declassification* decisions, in an attempt to change the view that national security was more important than other government responsibilities and that any possibility of harm, no matter how remote, to national security made information classified. Little evidence exists to show that these changes, directed for the most part at the overreaching national security mindset, had the desired effect. Throughout the Carter years the amount of information classified every year and the total amount of classified material continued to increase.[32]

2.3 Secrecy Under President Reagan

President Reagan reversed the trend toward tightening the classification rules in the current governing regulation, E.O. 12356,[33] which eliminated the requirement for identifiable damage for Confidential information, increased the number of categories applicable for classified information, eliminated automatic declassification, eliminated the balancing of public interest with national security in declassification decisions, and required the use of the higher classification in any dispute over the correct level. The effect of this order was to increase the ability (or inclination) of the government to classify information. The number of classification decisions rose dramatically after it. During the last years of the Carter Presidency classification grew about 1 percent a year, but in the first two years of President Reagan's new executive order, classification increased by an average of 11.5 percent a year.[34]

The most recent Congressional action in the area of classification is the Intelligence Identities Protection Act of 1982. The Espionage Act of 1917 contains general penalties for revealing classified information. The 1982 statute specified additional penalties for revealing the name of covert intelligence agents. It prevents people with authorized access to classified information that identifies agents from passing it on to anyone not authorized to receive classified information. Congress chose to accept the definition of classification used in the most recent executive order on classification.

In 1977, President Carter attempted to introduce a fourth level of information that needed safeguarding, Unclassified but Sensitive. Presidential Directive/National Security Council-24 (PD/NSC-24) gave the National Security Agency (NSA) responsibility for protecting both Classified communications and Unclassified but Sensitive communications related to national security. It gave the National Telecommunications and Information Administration (NTIA) responsibility for raising the awareness of users to potential national security problems.[35] Although PD/NSC-24 did not stimulate much criticism, its replacements, the National Security Decision Directive (NSDD; 1984) 145,[36] and its implementing regulation, the National Telecommunications and Information Systems Security Policy (NTISSP; 1986) 2,[37] both instigated a firestorm of protest. The protests centered on the requirement for civilian agencies to enforce the restrictions and the catch-all nature of the definition[38] of "Unclassified but Sensitive" as information that does not meet the definition requiring classification according to E.O 12356 but could cause damage to the national security if aggregated together. Examples included material such as the NTIS database or in the federal depositories. NTISSP 2 required all institutions, such as libraries, holding covered material to take precautions to prevent foreign nationals from access to it. Criticism by the civil liberties community and Congress led to rescinding these regulations. In March 1987, National Security Council director Frank Carlucci cancelled NTISSP 2, while Congress reversed NSDD 145 with the Computer Security Act of 1987.

2.4 Additional Secrecy Regulations

The secrecy system is more than only a classification system and is not limited to government-sponsored or funded information and technology. Individuals with no connection to government information can have secrecy restrictions placed on them. The AEA allows the government to classify information independent of any government involvement. This concept

was generalized in the Invention Secrecy Act of 1952, which permits the government to review all patent requests and classify any patent whose release may be detrimental to national security. This classification stands only for one year but may be renewed at the government's option. The provision applies to all patent applications, including those where the inventor has no knowledge of government information and the government has no financial interest.

Export control regulations allow the government to restrict any technology (or technical information), classified or unclassified, from export. These regulations include the Export Control Act, the Arms Export Control Act, the Trading with the Enemy Act, and the Export Administration Acts (EAA) of 1969 and 1979, the most far-reaching of these, which regulates U.S. exports to promote national interest, including restricting trade for national security reasons while expanding international trade for economic reasons. The dual goals of this law are highlighted by the Congressional findings that introduced it: "It is important for the national interest of the U.S. that both the private sector and the Federal Government place a high priority on exports." Congress also found that:

> The acquisition of national security sensitive goods and technology by the Soviet Union and other countries the actions or policies of which run counter to the national security interests of the United States, has led to the significant enhancements of Soviet bloc military-industrial capabilities. This enhancement poses a threat to the security of the United States, its allies, and other friendly nations.[39]

The EAA gives the president the ability to prohibit or curtail the export of any goods or technology.[40] Like classification, the Act, which includes classified and unclassified technology, offers] little guidance on what to control.

Notes

1. U.S. Congress. Senate. Subcommittee on Intergovernmental Relations of the Committee on Government Operations and the Subcommittee on Separation of Powers and Administrative Practice and Procedure of the Committee on the Judiciary. *Executive Privilege Secrecy in Government Freedom of Information Vol. 1.* Testimony of William P. Bundy. 93rd Cong., 1st sess., 8 May 1973, 269.

2. William G. Phillips, "The Classification System," in *None of Your Business: Government Secrecy in America*, edited by Norman Dorsen and Stephen Gillers (N.Y.: Viking Press, 1974), 63.

3. Harold C. Relyea, "Historical Development of Federal Information Policy," in *United States Government Information Policies: Views and Perspectives*, edited by Charles R. McClure, Peter Hernon, and Harold C. Relyea (Norwood, N.J.: Ablex Publishing Corp., 1989), 37; hereafter cited as Relyea.

4. 18 USC §793(a).

5. 18 USC §793(a)-(b).

6. Betty Houchin Winfield, *Two Commanders-in-Chief: Free Expression's Most Severe Tests*, John F. Kennedy School of Government Research Paper R-7, Harvard University, August 1992, 10.

7. Arthur Macy Cox, *The Myths of National Security: The Peril of Secret Government*, (Boston: Beacon Press, 1975), 35; hereafter cited as Cox.

8. Dallas Irvine, *Origin of Defense Information Markings in the Army and Former War Department*, Dec. 23, 1964, National Archives; quoted in Cox, 36.

9. E.O. 8381, 5 Federal Register 1147, March 26, 1940.

10. Relyea, 39.

11. E.O. 8381, 5 Federal Register 1147, March 26, 1940.

12. The concept of "born secret" might have outlived its usefulness. A DOE Sponsored group studying classification has recommended to the Secretary of Energy modifying the AEA to eliminate the "born secret" provision. Source: Roger Heusser, Dept. Director, Office of Declassification, DOE, phone conversation with author, March 4, 1994.

13. Relyea, 42.

14. E.O. 10104, 15 Federal Register 597, Feb. 1, 1950.

15. Relyea, 39.

16. E.O. 10209, 16 Federal Register 9795, Sept. 27, 1951.

17. Ibid.

18. Cox, 48.

19. E.O. 10501, 18 Federal Register 7049, Nov. 9, 1953.

20. Cox, 48-49.

21. Interview by the author with Michael Levin, NSA, Dec. 10, 1992.

22. E.O. 10964, 26 Federal Register 8932, Sept. 22, 1961.

23. Freedom of Information Revision, PL 95-454, Oct. 13, 1978.

24. Interview by the author with Marc Rotenberg, Washington Director, Computer Professionals for Social Responsibility (CPSR), Dec. 10, 1992.

25. E.O. 11652, 37 Federal Register 5209, March 10, 1972.

26. Ibid.

27. Ibid., §2.

28. Information Security Oversight Office, Department of Commerce *1992 Annual Report* (Feb. 16, 1993), 10.

29. Ibid., 18-19.

30. E.O. 12065, 43 Federal Register 28949, July 3, 1978.

31. Ibid.

32. Frederick Kaiser, "The Amount of Classified Information: Causes, Consequences, and Correctives of a Growing Concern," *Government Information Quarterly*, **6**, 3, 251.

33. E.O. 12356, 47 Federal Register 14874, April 6, 1982.

34. Kaiser, 251.

35. PD/NSC-24, Telecommunications Protection Policy (unclassified excerpts, Feb. 9, 1979), Nov. 16, 1977 (classified), quoted in U.S. Congress, Office of Technology Assessment, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information* (Washington, D.C., October 1987, OTA-CIT-310), 137.

36. NSDD 145, Sept. 17, 1984 (classified).

37. NTISSP 2, National Policy on Protection of Sensitive but Unclassified Information in Federal Government Telecommunications and Automated Information Systems, Oct. 29, 1986.

38. Hearing on Sensitive but Not Classified Information, U.S. National Commission of Libraries and Information Science, May 28, 1987, 21-22, 71-72.

39. 50 USC §2401.

40. 50 USC §2404.

Chapter Three

Why the Secrecy System Formed

> But whenever, armed with new means, we put our thumbs on one of Fate's many balances, we tip that balance one way or the other.
>
> Anthony G. Oettinger[1]

3.1 Cold War Assumptions

The reasons for the way that national security mindset and its accompanying secrecy system developed lie in the military, economic, and social environment following World War II. The national security strategy was based on perceptions about the strengths and weaknesses of both the United States and the Soviet Union, that is, about U.S. technological advancement and economic power versus Soviet military size. Because technological advantages, owing to their short life cycle and their susceptibility to technology transfer, were more fragile than size, secrecy was a necessary component of the national security strategy chosen to fight the Cold War.

In the 1940s, the Soviet Union had a perceived advantage in conventional warfare in Europe because of its larger standing armies, its greater number of conventional weapons, and a theater of operations that lay closer to its border. It also had a closed political system that could allocate a larger percentage of the budget for weapons. By the end of that decade, it possessed rudimentary nuclear weapons but not the delivery system necessary to threaten the U.S. directly. Although its large work force was capable of producing vast quantities of weapons, its economy had been badly damaged by the War and required rebuilding.

The U.S. had perceived advantages in nuclear weapons and delivery systems and extensive scientific and technologic expertise. Its economy was robust, undamaged by the War, whereas the War left the economies of other major countries in disarray. With excess industrial capacity, the U.S. established a position of global economic leadership. Rapid technologic innovation, stimulated partly by the need for high-technology military equipment, soon improved product quality in many sectors of the economy. In general, U.S. military technology was superior to that of Soviet weapons systems, although some Soviet technologies were equal to those of the U.S.[2] Theoretically, the U.S. needed fewer weapons than the

Soviets to accomplish the same military objectives, so it was to the economic advantage of the U.S. to build, and staff, fewer but superior weapons and use more resources for commercial enterprises. The costs and benefits of a smaller, high-technology army were perceived to be greater than those of a larger, low-technology army, but the margin of error was small.

A high-technology military has direct consequences on secrecy requirements. Large standing armies offered one distinct advantage: for another country to match the size quickly would be difficult. The Soviet Union did not need to worry that the U.S. would modify its own strategy to be able to match Soviet troop levels or number of weapons systems. Advanced technology, however, is eventually lost to an adversary, who may reinvent it, buy it from another source, or steal it. Because the western allies were not the only ones involved in scientific progress and because stealing technology is easier and cheaper than inventing it, the Soviets could continually upgrade its military with the latest military technology. The U.S. could at best delay Soviet acquisitions and drive up the cost to the U.S.S.R. Once committed, the U.S. could not change strategy. It had the dual problem of delaying Soviet acquisition of available technology while also continuously inventing new technology.

The U.S. strategy demanded protection of its own technological advantage. The Soviet Union could not be allowed to gain an equal technological footing or the larger Soviet military might become decisive in a conventional war. Because the U.S. government did not know what particular information or technology would help the Soviets, especially at the outset, it imposed secrecy on a wide variety of information and technology, including much without direct military application. The task of protecting American information and American-developed technology was complex and required stronger security measures than those used before the Cold War. New mechanisms had to be developed, regardless of their economic or societal implications, and those developed in the early years of the Cold War still constitute the current secrecy system. At the same time that the government was protecting technology, it also needed to ensure that technology, both applied defense technology and basic science, would continue to advance. The improvement of technology required a large investment in research. Beginning in the early 1960s defense R&D averaged $30 billion a year (in 1990 dollars), increasing to more than $40 billion a year in the middle 1980s, while overall federal research grew from $40 billion to $60 billion.[3]

3.2 Post-Cold War Assumptions

Many Cold War assumptions about national security no longer hold in the 1990s. New ways of looking at the world need to be incorporated into post-Cold War national security policy.

The apparent stability introduced by the bipolar Cold War has disintegrated into regional strife. No enemy directly threatens the U.S., and whether current regional conflicts threaten national security even indirectly is debatable. Determining which conditions constitute a threat to the U.S. and which types of reactions enhance its national security interests are among the important questions that need answering in a security policy.

Economic assumptions also have changed. The U.S. economy, while still the world's largest, no longer maintains the dominance it enjoyed immediately after World War II. The world economy is increasingly international and intertwined. Most large defense corporations are multinationals, with much of the manufacturing and research conducted outside the U.S.. Technology development has become so expensive that advanced technology is more and more created through alliances of multinational firms, both U.S. and foreign. Foreign ownership of American-based firms has increased. U.S. dependence on other countries—for basic raw materials, capital with which to finance public and private debt, and military technology[4]—reflects this international economy. The budget deficits limit the amount the U.S. can afford to spend on defense, and much of the planned deficit reduction will come from defense cuts. Smaller budgets may force a shift from a policy of absolute security toward one of adequate national security. An example of this changing philosophy can be found in the recent force structure study. some argued that the U.S. security required it to be able to fight two Desert Storm sized wars simultaneously, while others argued that it was adequate to be able to fight one war and a holding action simultaneously.

The international community has begun to assume a larger role in global security, and the parts played by established international organizations, such as the United Nations or the International Atomic Energy Agency (IAEA), are expanding. Some examples of peacekeeping efforts or sanctions imposed by the UN during the 1990s include Desert Storm, imposition of no-fly zones in Iraq and Bosnia, and humanitarian operations in Somalia and Cambodia. In 1993, the IAEA stepped up inspections of suspected nuclear sites in Iraq and North Korea.

While unilateral U.S. action is still possible, the U.S. has been working under UN auspices to gain international cooperation for its security objectives. In the Gulf War and Somalia, for example, the U.S. acted as part of a multinational force.

Civil liberties sensitivity within the U.S. also has increased since the end of the Cold War. Now that fear of a Soviet attack no longer overshadows all other issues involving secrecy, those related to traditional liberties—such as government openness, freedom of the press, and personal privacy—have arisen. Release of government information, particularly that formerly classified, no longer seems potentially so damaging as during the Cold War. Conversely, society has become more sensitive to the need for information privacy from both government and commercial activities.

The importance of military funding for technology development declined in the 1980s. In many important military technologies, such as computers and communications equipment, commercial technology is generally superior to military technology. The paradigm of military spinoff has changed to commercial "spin-on."[5] The military uses many commercial products, because they perform better, have a lower cost, and are developed in less time than those produced by and for the military. Even formerly exclusively military technology such as cryptography has commercial uses for commercial security and privacy products.[6] As commercial interest in military technology increases—and as commercial R&D independently discovers many of the government's most important secrets—the government lead in the technology will be reduced.

Technology for providing information to the public improved in the late 1980s. Information providers now can bypass traditional government "censorship" to provide information previously unavailable quickly and cheaply, as, for example, the instantaneous coverage of the Gulf War from Iraq versus the limited coverage from Saudi Arabia allowed by the military. Reporters in Baghdad could transmit "information" directly through commercial satellites onto television screens throughout the U.S. The government could not control this information stream, although it was concerned about the propaganda effect of these reports. Even though reporters in Saudi Arabia had the same communications equipment, government controls limited what they were allowed to broadcast. Advanced

telecommunications technology makes it harder for government to control, and potentially manipulate, the flow of information to the public.

Many agencies of the U.S. government are concerned with various aspects of secrecy and often come into conflict over specific decisions. Agencies such as the departments of Defense and Commerce have different missions and responsibilities and do not always agree about the "correct" way to balance competing needs. For issues such as export control, the Defense Department's view of technologies that could damage national security is stricter than that of Commerce. Competing missions prevent the government from responding to those issues with a monolithic national security viewpoint.

3.3 Secrecy Restrictions

Secrecy restrictions, which cover many areas, are not abstract principles but affect the daily lives of U.S. citizens. The effects of secrecy include higher costs or unavailability of products owing to limitations on technology development, uninformed public debate because of restrictions on information flow, or loss of investment profitability through limitations on industry.

Most of the secrecy mechanisms implemented by the government during the Cold War had considerable impact, sometimes detrimental, outside the national security arena, including such secrecy mechanisms as the following:

(*i*) *The formal classification system.* This system creates the foundation for information secrecy. The government can unilaterally decide, for national security reasons, to restrict access to certain information. The Espionage Act (1917) and related laws established severe penalties for unauthorized release of classified information (see **Chapter Four**).

(*ii*) *Export control.* Such control provides a basis for technology secrecy. The government can restrict, either unilaterally or in concert with allies, the export of any technology (including information about the technology) to any country in the world. Since much of the technology on the export control lists consist of dual-use technology, export control has a considerable impact on commercial industry (see **Chapter Five**).

(*iii*) *Foreign Direct Investment (FDI) limitations*. The International Emergency Economic Powers Act gives the president the right to restrict ownership of U.S. firms. The government, through the Committee on Foreign Investment in the U.S. (CFIUS), reviews proposed foreign acquisitions of U.S. companies for national security and technology transfer concerns. Unlike other secrecy restrictions, criticized as too restrictive, FDI concerns are most commonly criticized for their ineffectiveness; critics would like to see more acquisitions rejected and protection of the U.S. industrial base increased[7] (see **Chapter Seven**).

(*iv*) *Secrecy patents*. The Invention Secrecy Act allows the government to classify any patent application, even when the government has no claim on the technology developed. The law prohibits the inventor from publishing information about the technology or discussing it with uncleared people. Although the government may permit the inventor to use the technology in a commercial product, the product has no patent protection.[8] More than five thousand secrecy orders were in effect in 1991, with seven hundred new orders issued each year from 1989 to 1991. Although most secrecy orders are on government-owned technology, hundreds are still placed on private inventions[9] each year, including in 1991 506 secrecy orders on private individuals or companies.[10]

(*v*) *Media restrictions*. One way to influence public debate is to control the information available to the public. An example is limitations on military reporting in the 1980's. On site coverage, by its very nature, can be controlled by military refusal of access by the media to the war zone. Starting with the Grenada invasion in 1983, access by the press to the military was sharply limited. The press was excluded, nominally for reasons of secrecy and safety.[11] The media criticized the government, out of the fear that if the military held exclusive control over information, it could manipulate public debate by selective release.[12] The criticism caused the military to set up a press pool system, supposedly to supply an initial, independent assessment of military action. The pool was used in Panama (1989) and the Persian Gulf (1990–91), but questions about the availability of information to the people remain (see **Chapter Eight**).

(*vi*) *Restrictions on unclassified scientific communications*. In the late 1970s and early 1980s, the government identified unclassified scientific research as technology transfer channels that should be controlled. Restrictions included the exclusion of foreign scientists

from conferences, withdrawal of technical papers from conferences, limitation of the actions of foreign scientists at U.S. universities, imposition of secrecy orders on technical research,[13] barring unlicensed receipt of foreign periodicals, restrictions on publication of research by U.S. scientists in foreign journals, and application of export control laws to scientific writing.[14] Predictably, the scientific reaction has been that these are unwarranted intrusion on important American values (see **Chapter Eight**).

(*vii*) *Congressional restrictions*. Except for a few specific areas, the classification system is controlled by the executive branch. Because controls on the release of information extend to Congress, the president, at sole discretion, can restrict Congressional access to classified information. The limits range from allowing Congress access to information, placing procedural restrictions on access, allowing only selected members of Congress access to information, or denying Congress access.[15] Congress, basically an open institution, cannot freely use classified information in public debate as part of its oversight responsibilities. Excessive classification reduces the ability of Congress to oversee the national security establishment.

(*viii*) *Defense conversion*. Prior to 1980, there was little incentive, and many national security disincentives, for the national security community to transfer technology to the commercial sector. Starting in 1980 with the Stevenson–Wylder Act, Congress, looking to commercial benefits, began actively to promote defense technology conversion. In the 1990s, with economic competitiveness an even more prominent national objective, commercializing defense technology by removing its secrecy is gaining importance (see **Chapter Seven**).

(*ix*) *Limitations on commercial technology*. The government becomes concerned when industry commercializes military technology such as cryptography. Once exposed, the technology will be available to other countries and might adversely affect national security. Hostile countries could use the technology against the U.S. or use its knowledge to develop countermeasures to U.S. equipment. Several mechanisms have been used to slow down or prevent commercialization, including secrecy patents, limitations on basic research grants, attempts to impose self-regulation on researchers,[16] the development of circumscribed technical standards, the placement of export controls on products, and the definition of legal limits on the strength of the product[17] (see **Chapter Six**).

(*x*) *Secret Executive Directives*. Presidential national security regulations are routinely classified and withheld from both public and congressional scrutiny.[18] Many of these directives constitute intelligence findings and are properly classified. Many such presidential directives, however, deal with the missions and responsibilities of the government's national security agencies and the way they operate. Under President Bush, classified directives dealt with such basic issues as space policy, telecommunications, Soviet immigration policy, and counter-narcotics efforts.[19] Other directives treated far-reaching and controversial political questions, such as NSDD 145, which delegated the protection of Unclassified, but sensitive information to the defense department. The practice of classified executive orders precludes informed debate or oversight on the activities of the national security community.

(*xi*) *Secrecy agreements*. According to NSDD 84,[20] every government employee with access to classified information must sign a secrecy agreement requiring them to submit any material dealing with what they learned while in government service for prepublication review. Critics claim that the secrecy agreements are used as much to silence critics of the government as to prevent classified information from being released.[21] Secrecy agreements were upheld as constitutional in U.S. v. Snepp (1980)[22] and U.S. v. Marchetti (1972)[23] (see **Chapter Eight**).

Notes

1. Anthony G. Oettinger, *Whence and Whither Intelligence, Command and Control? The Certainty of Uncertainty* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, 1990, P-90-1), 15.

2. National Academy of Science, *Balancing the National Interest U.S. National Security Export Controls and Global Economic Competition* (Washington, D.C.: National Academy Press, 1987), 48. In 1987, the Defense Department identified seven significant military areas in which Soviet technology equalled U.S. technology, out of a total of twenty areas reviewed. The areas included: aerodynamics and fluid dynamics, conventional warheads, laser weapons, electro-optical sensors, nuclear warheads, optics, and power sources.

3. John A. Alic et al., *Beyond Spinoff: Military and Commercial Technologies in a Changing World* (Boston: Harvard Business School Press, 1992), Table 4-1, 89, and Figure 4-2, 94. U.S. Defense R&D grew to $43 billion in 1988.

4. Raymond A. Gauger et al., *US National Economic Security in a Global Market* (Cambridge, Mass.: John F. Kennedy School of Government National Security Program Discussion Paper 90-03, Harvard University), 1990. This paper describes very well what foreign dependency means to the U.S. military; one example used is the reliance of defense technology on foreign—especially Japanese—semiconductors.

5. Alic et al., *Beyond Spinoff*, 1-26.

6. *INFOSECURITY News*, May-June 1993, 51-56. A quick look at the new products sections shows many products now being introduced that contain commercial cryptography, including, among others, MultiNet Authentication, OCSG/Kerberous for the Macintosh, A6000-IBM Network Security Processor, 656 Crypto Pump, Intelligent Security Card, and CryptCard.

7. Bureau of National Affairs, Inc., "'Major Reforms' in Monitoring Defense-Related Acquisitions Urged," *International Trade Reporter* (August 19, 1992). [NEXIS]

8. Transcript of "Show: Morning Edition," National Public Radio Morning Show, Sept. 14, 1992, *National Public Radio*. Ken Cage.

9. Ibid. Steven F. Aftergood, "The Perils of Government Secrecy," *Issues in Science and Technology* (Summer 1992), 85.

10. Aftergood, ibid.

11. Jack Gottschalk, "American Military Press Censorship," *Communication and the Law*, 8, 4 (Summer 1983), 49; reprinted in *1984: Civil Liberties*, 463-480.

12. Drew Middleton, "Barring Reporters from the Battlefield," *The New York Times Magazine*, Feb. 5, 1984; reprinted in *1984: Civil Liberties*, 502-505.

13. George Davida and Peter Magrath, testimony reprinted in *1984: Civil Liberties*, 51-58, 90-92.

14. Mary M. Cheh, "Government Control of Private Ideas," in *Striking a Balance: National Security and Scientific Freedom First Discussions*, edited by Harold C. Relyea (Washington, D.C.: American Association for the Advancement of Science, Committee on Scientific Freedom and Responsibility, 1985), 6.

15. Patsy T. Mink, *The Freedom of Information Act*, 81-85. Congresswoman Mink sued the Environmental Protection Agency (EPA) under the Freedom of Information Act to obtain classified document about environmental assessments of nuclear tests denied her Congressional committee. The Supreme Court denied the petition.

16. In the early 1980s, NSA instituted a voluntary review process for academic cryptographers: before publishing a paper dealing with cryptography, the researcher submits it for NSA review.

17. The Land Remote-Sensing Commercialization Act of 1984, PL 98-365, 98 Stat. 451, 15 USC 4241, requires government licensing of commercial satellites, which allows the government to control the technical capabilities of any satellite.

18. Steven Aftergood, "Secret Presidential Directives," *Secrecy and Government Bulletin* (October 1992), 15, 2. This policy may be changing slightly under President Clinton whose first two presidential directives signed were unclassified and released. See Aftergood, "New Presidential Directives Disclosed," *Secrecy and Government Bulletin* (April 1993) 21, 1.

19. Aftergood, "Perils of Government Secrecy," 82. Even the number of National Security Directives issued by President Bush is classified.

20. National Security Decision Directive 84, "Presidential Directive on Safeguarding National Security Information," March 11, 1983.

21. Ralph McGehee, *1984: Civil liberties*, 45.

22. Snepp v. United States, 444 U.S. 507 (1980).

23. United States v. Marchetti, 466 F.2d 1309 (4th Cir.).

Chapter Four

Classification

> The Task Force noted 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, but agreed that in spite of the great advantages that might accrue from such a policy, it is not a practical proposal at the present time. . .within the current framework of national attitudes toward classified Defense work.
>
> Defense Science Board Task Force on Secrecy[1]

4.1 President Reagan's Executive Order 12356

The formal classification system[2] that underlies the secrecy system has not been modified since the administration President Reagan, whose view of the Soviet Union as an "evil empire" was a remnant of the Cold War, and the threats it was intended to counter have been replaced by new national priorities. To address the question of whether the classification system still meets today's new threats requires understanding its strengths and weaknesses, as well as its costs. This chapter reviews in detail the present system and its implications.

Executive Order 12356,[3] issued by Reagan in April 1982, defines the current executive department classification system and provides the authority for most classification decisions. Supplemental classification regulations, such as the Atomic Energy Act of 1946, resulted from Congressional action. The specific details, as well as the basic tone of the system, provide insights into the national security priorities at the time the order was written.

E.O. 12356 identifies two types of classification decisions, *derivative* and *original*. *Derivative classification* permits federal employees with security clearances to classify information by applying prior classification decisions when the "information is in substance the same as information currently classified"[4] or by following predefined rules.[5] This process relies on previous decisions and should not allow the classifier any discretion. In reality, information seldom falls neatly into classified or unclassified categories which could be easily used for derivative classification. Decisions about the proper classification of specific data must often be made prior to the application of a derivative classification. A common mistake

is classifying derivative data with the highest classification of the original information, regardless of their true classification.[6]

Original classification decisions are necessary in the absence of guidelines that would define the proper classification of information. Classification requires three steps: (*i*) The person making the classification decision must have original classification authority for the classification level. Original classification authorization is limited to "the minimum [officials] necessary to administer" the executive order and they must "have a demonstrable and continuing need to exercise this authority."[7] (*ii*) The information or technology must qualify under a predefined category, including:

1. Military plans, weapons, or operations
2. Vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security
3. Foreign government information
4. Intelligence activities (including special activities) or intelligence sources or methods
5. Foreign relations or foreign activities of the U.S.
6. Scientific, technological, or economics matters relating to national security
7. U.S. government programs for safeguarding nuclear materials or facilities
8. Cryptology
9. A confidential source
10. Other categories of information relating to the national security that require protection against unauthorized disclosure as determined by the President or by agency heads or other officials delegated original classification authority by the President.[8]

If the information or technology falls within one of the defined categories, the potential national security damage must be determined. Information can be classified at three levels:

- "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security

- "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security

> • "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.[9]

Information can also be classified if disclosure in the context of other information causes harm. Unauthorized disclosure of foreign government information, identity of a confidential foreign source, or intelligence sources and methods are "presumed to cause damage to the national security" automatically meet the test for Confidential[10] and give the government wide authority for protecting the information.

The executive order mandates that information remain classified as long as it meets the outlined conditions without providing comparable direction about declassifying information. Declassification can occur in two ways: (*i*) a declassification date or event can be supplied by the original classifier or by a manual review, as for example, during a FOIA request; or (*ii*) information can be reclassified, even if publicly available, if an official with original Top Secret classification authority determines that such classification meets the requirements of the executive order and that the information may be reasonably recovered.[11]

The executive order provides some general prohibitions against classifying; classification shall not be used :

> (a) to conceal violations of law, inefficiency; or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security. (b) Basic research not clearly related to national security may not be classified.[12]

4.2 Criticisms of the Classification System

Because the classification system affects many aspects of American society, it has been a lightning rod for criticism. Primary criticisms of the system include using classification to limit civil liberties, unnecessarily expanding the scope of national security, ambiguous classification regulations, and faulty implementation. These criticisms are recurring problems. Early studies of classification, starting in the 1950s, by the national security community identify essentially the same problems.[13] Successive presidents since Eisenhower have tried to reform the system, but implementation problems remain. Many people believe that the modifications instituted under E.O 12356 exacerbate the basic problems, such as the tendency

to overclassify, because the order removed the counterweights to classification in President Carter's order.[14]

4.2.1 Excess Scope

Many critics think that the classification system extends the scope of national security too widely and supports a national security mindset prejudicial to civil liberties. [Through World War II, secrecy was reserved for unambiguously military or foreign policy information. Owing to their narrow scope, national security restrictions had little impact on the average citizen, but during the Cold War national security embraced large sectors of U.S. society. Because of their ubiquitous nature, during the Cold War national security restrictions affected the civil rights of average citizens.

Secrecy assumes that the national security need to protect information outweighs other rights, such as informed public debate, whenever they conflict. Civil libertarians hold the opposite view, that the U.S. is an open society whose citizens have a fundamental right to know about government actions, a right to be abridged only in the most serious circumstances. The battle between these philosophies about government information policy raged throughout the Cold War.

A number of mechanisms with implications for civil liberty use classification as a tool to control information. These include protecting defense information from Congressional oversight[15] by classifying the information, secret executive orders,[16] selected government leaks of classified information,[17] secrecy orders on government employees,[18] and by prior restraint on publishing.[19] Because the goal of national security was so important and the damage to civil liberties unquantifiable, the general public usually supported the president in any disputes.

Critics claim that missing from the classification system was the recognition that a proper balance between national security and other national goals served any useful purpose. The government treated national security as the primary goal during Cold War, when all other national objectives were secondary and were accomplished only if they did not interfere with national security. The government did not acknowledge that while parts of national security needed that priority, the scope was so large that the national security umbrella covered many

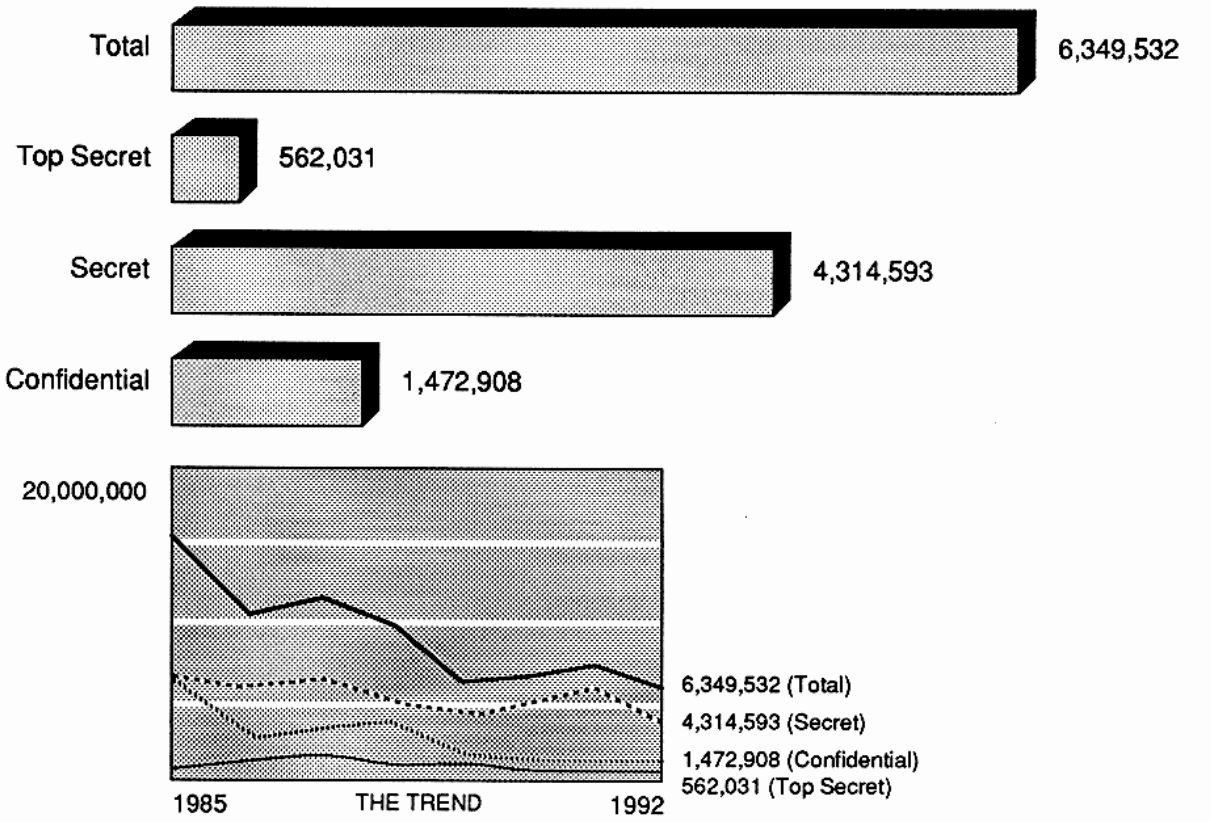
areas of lower priority. Overall, national objectives might have been better met if those items of lesser priority had been balanced with other national objectives.

4.2.2 Overclassification

One of the most persistent criticisms[20] of the classification system is the large volume of classified material that either does not meet criteria for classification or the overclassification of information higher than permitted by those criteria. Large inventories of incorrectly classified material increase the costs for its handling, storage, and protection, as well as for prevention of its being made public. Recent government documents show that the overall scope of overclassification may be decreasing due to a downward trend in classification decisions. The government reported 6.4 million classification decisions. The government reported 6.4 million classification decisions in 1992, down from 15 million in 1985 and 7.1 million in 1991. Figure 4-1 shows the specific breakdown. An indication of continued overclassification however is the comparatively frequency of each type of classification decision. Nine percent of the documents were classified Top Secret that year, but 68 percent were classified Secret.[21] It would seem that the classification definition, which places increasingly difficult requirements at each succeeding level, would result in more Confidential than Secret documents, yet Secret classifications decisions outnumbered Confidential classifications by almost three million. The following are some causes of overclassification.

(*i*) *Ambiguous and arbitrary classification rules*. The rules, which allow individual interpretations by not defining a consistent test for deciding the proper classification, lend themselves to overclassification. The categories defined by E.O. 12356 can be very broadly interpreted; for example, one of the seemingly more straightforward categories, intelligence methods and sources, has been accepted by the courts as authorizing everything from traditional intelligence sources to the classification of law enforcement techniques originated by the intelligence community. Nothing in the executive order permits law enforcement methods to be classified.[22] The definition also contains a catch-all category that allows classification of anything that an original classification authority deems necessary, effectively negating the usefulness of categories as a limiting factor. No accepted definition exists of the meaning of "damage to the national security," the determination necessary for classification, a situation that permits inconsistent subjective interpretations. For example, the National Security Archives, a private organization that collects declassified documents for research

purposes, often, through FOIA requests, receives multiple copies of the same document declassified by different agencies. Frequently, in different copies different sections are declassified, making reconstruction of the original possible.[23] Because the criteria for making classification decisions are ambiguous, classification of any specific information becomes somewhat arbitrary and improper classification or overclassification of data an almost inevitable consequence. One solution to this problem is to have detailed guidance about the meaning and scope included as part of each classification decision. In practice, this is seldom done. Classification decisions, usually in the form of a classification guide, define specific information and technology as classified, but do not explain the reasons for the decision. People using the guides later have little basis for deciding the proper classification of information which does not precisely fit a predefined category.



Source: Information Security Oversight Office, 1992 Report to the President (Washington, D.C.: General Services Administration, Feb. 16, 1993), 16.

Figure 4-1

Classification Activity for 1992

(*ii*) *Human tendencies promote overclassification.* Inherent in the definition, damage to U.S. national security is caused by the release of material that should be classified. The overclassification of material appears to do no immediate, discernible damage to the U.S. Although critics argue that in the long run exclusion of the information from the public debate often causes as much or more damage as the release of information, the damage is impossible to quantify. The natural reaction of people faced with classification decisions is to err on what they see as the safe side and classify borderline material to prevent foreseeable damage. The ingrained national security mindset and the bureaucratic feeling that "knowledge is power"[24] reinforces the tendency to play safe. Little institutional support exists for individuals to be open. E.O. 12356 1.1(c) further strengthen this tendency by specifying that "if there is reasonable doubt as to the need to classify or the appropriate level of classification, it should be safeguarded as if classified at the higher level until a determination by an original classification authority." The government disagrees that overclassification represents a large problem. The Information Security Oversight Office (ISOO), charged with overseeing the classification system, reports that in 1992 only 5 percent of inspected documents were overclassified.[25]

(*iii*) *No (enforced) penalties for overclassification.* Although the penalties for releasing information that should be classified are significant,[26] there are no corresponding penalties for overclassification. E.O. 12356 specifies administrative penalties, from a "reprimand to loss of access to classified information, for knowingly and willfully classifying or continuing the classification of information in violation of the executive order,"[27] but they are not enforced. Few federal employee has ever been officially sanctioned for overclassification.[28] Without meaningful penalties for overclassification, but with those for not classifying (and releasing) information rigorously enforced, the tendency to overclassify information is further strengthened.

(*iv*) *Lack of training.* Lack of employee training in the classification requirements[29] is one of the primary reasons for overclassification, contributing to the problem of personal interpretation. Original classifiers, ordinarily senior people, have little time to learn the classification system. Derivative classifiers, who make the bulk of classification decisions, receive no training at all. An exception is the Department of Energy (DOE) which requires

each classifier to take classes and be certified prior to getting original classification privileges, as well as undergo periodic audits of their performance.[30]

4.2.3 Executive Definition of Classification

Classification policy has been promulgated through executive orders, not congressional action.** Where Congress does address the issue, as in the Freedom of Information Act, it allows secrecy where "specially authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and are in fact properly classified pursuant to such Executive order."[31] Classification authority puts a great deal of power for controlling public debate in the hands of the executive branch, including determination of Congress's own access to classified information. Given the difficulty of defining a law that is both useful and flexible enough to adapt to changing circumstances, Congress's reluctance to legislate classification is understandable. Because Congress must abide by executive restrictions on access and on handling of classified information, the classification authority of the executive branch could tempt it to manipulate the classification definition, or specific classification decisions, to hide politically embarrassing actions from Congress.

4.2.4 Lack of Declassification Procedures

Damage to the U.S., the underlying basis for classification, depends on a number of issues, including the passage of time. Information loses some or all of its sensitivity after the passage of enough time. Thus, information, properly classified today, does not remain properly classified indefinitely. The problem is determining when the information stops being sensitive and can be safely released. Periodic review is the safest way to determine if the classification remains valid, but the tremendous volume of material makes periodic review impractical. The number of classified pages is so large that Steven Garfinkel, Director of the ISOO, does not know the amount of classified information in existence and says that it would be too expensive to find out.[32] The National Archives, responsible for declassifying historical documents, estimated that at the end of 1992 it had at least 325 million pages awaiting declassification.[33] Declassification does occur—ten million pages in 1992,[34] sixteen million

---

**Bills introduced by Representative Glickman and Senator DeConcini on March 2, 1994, would put classification on a statutory basis. Among other provisions, it would eliminate Confidential as a classification and require quick declassification of most material (*Baltimore Sun*, "Bills Would Count Number of Classified Documents," March 3, 1994, 5).

in 1991[35] declassified by various agencies—but the total amount of material continues to increase because the process cannot keep up with the avalanche of new material.[36] One attempt to alleviate this problem—eliminated by President Reagan—was automatic declassification, which required information, unless specifically exempted, gradually to be reduced in classification level until declassified after a set number of years determined by its original classification. The specific number of years decreased from twelve under Kennedy[37] to six under Carter.[38] Although declassification regulations were often abused,[39] they provided a mechanism to prevent indefinite storage of classified information. The current system of declassification frequently requires a manual review, which is an important reason for overclassification.[40]

4.2.5 Too Many Levels of Classification

Several studies have recommended elimination of Confidential[41] to simplify the system and reduce the amount of classified material. Reasons cited include overuse of the classification level and its restriction on the free exchange of scientific and technological information.

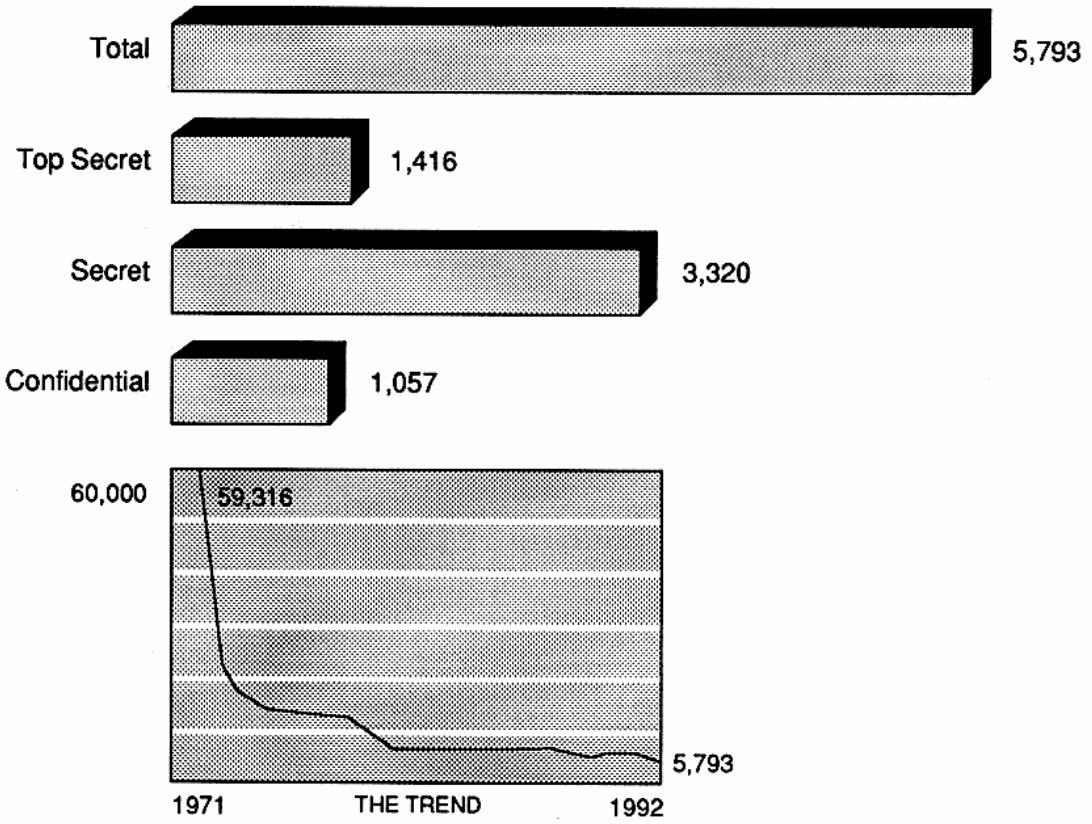
4.2.6 Too Many People with Classification Authority

Although the classification system is changing, a major criticism of it, especially in the 1950s, was that too many people had classification authority. At the end of 1992, 5,793 individuals in the executive agencies had original classification authority, including 1,416 with Top Secret authority[42]; in contrast, in 1971, sixty thousand had classification authority.[43]

Figure 4-2 shows the variations in the number over time. Although from a historical perspective the number is quite low, allowing so many people classification authority makes any development of consistent classification standards difficult.

4.2.7 Classification for Political Purposes

The current system can be manipulated by the administration and Congress for political purposes. Information drives public debate. The leaking of selected classified information by senior politicians, both in the executive branch and in Congress, can easily distort public



Source: Information Security Oversight Office, 1992 Report to the President (Washington, D.C.: General Services Administration, Feb. 16, 1993), 10.

Figure 4-2

Classification Authority for 1992

perception of issues in ways that benefit the leaker. Contrary information remains classified and out of the debate. Although such practice is not limited to military debates, obvious examples occur in almost any debate about military requirements and weapon systems.[44]

4.3 Comparison with the Official Secrets Act (1989)

Although the U.S. classification system has been criticized, restrictions on access to information in other countries are even tighter. The Official Secrets Act of the United Kingdom, considered an open, democratic society and the closest ally of the U.S., defines

stringent criminal penalties for releasing unclassified government information. Revised in 1989,

> [the] Official Secrets Act 1989 identifies six specific areas of information in which the "public interest" needs to be protected by the criminal law, being:
> (1) Security and Intelligence;
> (2) Defence;
> (3) International relations;
> (4) Crime and special investigation powers;
> (5) Information resulting from unauthorized disclosures or entrusted in confidence;
> (6) Information entrusted in confidence to other States or international organizations.[45]

The 1989 revision removed provisions of the 1911 and 1920 versions to the effect that any dissemination of official information represented a betrayal of trust, and they substituted provisions (5) and (6). It also added the need for the government to prove "specific harm" before criminal sanctions apply. Release of intelligence information and other national security information does not require a harm test.[46] Many of these provision are similar to U.S. laws, but some are more restrictive; for example, compare this Act with the Espionage Act, which limits its scope to purely military information.

4.4 Benefits of Classification

The preceding criticisms should not be taken as a blanket condemnation of classification. U.S. security requires protection of national security information, and even the most vociferous critics of the system agree that security requires some type of classification. The specific benefits of classification are unfortunately very hard to quantify. Classification contributes to wide-ranging objectives—delaying the acquisition of technology by adversaries, delaying countermeasures against weapon systems, achieving battlefield surprise, protecting international negotiations, protecting intelligence, and sharing information with foreign governments. The national security community, as currently constituted, could not operate without a robust classification system.

The benefits of classification are partly dependent on the national environment. Changes in the environmental assumptions change the type and amount of sensitive information as well as the degree of secrecy necessary. The question is not one of the need for classification policy but of its proper scope in the new environment.

4.5 Costs of Classification

Although the protection of sensitive information provides an enormous benefit, classification also imposes a significant cost. The benefits of protecting specific information change with the world situation, whereas the costs depends strictly on the volume and classification level of the information. Unfortunately, due to a lack of reporting mechanisms, the government does not have good figures on the systems' total cost.[47]

4.5.1 Direct Costs

The direct costs of the classification system, proportional to the amount of classified information, can be enormous.*** The Department of Defense (DOD) estimated that in 1989 the cost of protecting classified material in industry was $13.8 billion.[48] Any substantial reduction in the volume of classified material could cut these costs considerably. Direct costs of classification include the cost of clearing employees (and the periodic review of these clearances), processing current material, protecting material in storage (including specialized construction, guards, and safes), protecting information during transmission (military-grade cryptographic devices, armed couriers), and additional overhead in military contracts to cover the National Industrial Security Plan.

4.5.2 Indirect Costs

Besides the direct costs, there are unquantifiable indirect costs related to the impact of classification system on economic competitiveness. These include loss of efficiency while working with classified material, the establishment of barriers between nations, the creation of uncertainty in the public mind on policy issues, impediments to the flow of scientific and technical information within the U.S. and abroad,[49] and a slowing of the conversion of military technology to commercial products.

Scientific and technical communication is especially vulnerable to secrecy. Critics of the system have argued that classification has slowed the progress of U.S. technological improvement by eliminating necessary channels of scientific communication.[50] The Defense

---

***The DOE rule of thumb is that approximately 10 percent of the cost of each classified program is because of the classification, according to Roger Heusser.

Science Board Task Force on Secrecy, in a 1970 study of the classification system, observed that:

> it is unlikely that classified information will remain secure for periods as long as five years, and it is more reasonable to assume that it will become known by others in periods as short as one year through independent discovery, clandestine disclosure or other means. . . . 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 engendering frustrations. 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. . . In the opinion of the Task Force, the volume of scientific and technical information that is classified could profitably be decreased by perhaps as much as 90 percent.[51]

4.5.3 Social Cost

The social cost of classification can be found in the development of the national security mindset and the anti-government distrust engendered in its opponents. Classification is a bureaucratic procedure, limited to national security information, but a substantial percentage of the public believes that the government abuses the system to protect information that the executive branch does not want released.[52] During the 1970s, in response to the Vietnam War and Watergate, there were many calls for reform. That sentiment was also voiced by critics within the government, as shown by the following statement by Morton Halperin, formerly of the American Civil Liberties Union, a Deputy Assistant Secretary of Defense under President Johnson, and nominated by President Clinton (although he withdrew in January 1994) as Assistant Secretary of Defense for Democracy and Human Rights:

> In the aftermath of Vietnam and of Watergate it appears that secrecy has been neither a rare nor a benign phenomenon. On the contrary, the executive branch has made secrecy an essential part of its modus operandi, and the reasons are far more complex than the traditional rationale of national security implies. The Pentagon Papers showed how successive administrations kept Congress and the public in the dark about vital foreign policy decisions. . . . Congress and members of the public came to feel that they had been systematically excluded from decisions of the utmost importance, decisions they had a constitutional right to participate.[53]

Later examples lend credence to the fear that classification is still sometimes used to prevent oversight of the executive branch. Examples from the 1980 and 1990s are Iran Contra, where the executive branch failed to provide the Congressional Intelligence

committees the information on the covert action required by law, and the BNL investigation. Representative Henry Gonzales said of the second case "The roadblocks the administration has put in the way of my investigation of the Banca Nazionale del Lavoro (BNL) . . . lead me to conclude that the administration has engaged in a high-level effort that has included improperly classifying embarrassing material."[54]

Although the government claims that their review procedures would catch any widespread abuse of the classification system,[55] public perception about the lack of accountability is a major question with which the administration still has to come to grips. As long as the government apparently operates with excessive secrecy certain segments of the country will continue to distrust the government.

4.6 Post-Cold War Classification

The current classification system is probably on its last legs. Two studies in the early 1990s looked at how well the classification system meets the new environment. Director of CIA Robert Gates created a task force to review secrecy and classification.[56] Since the Clinton administration took office, a joint CIA-DOD task force on post-cold war security issues, including classification and secrecy. Their report was published in March 1994.[57] A draft of new executive order on classification was circulated for comments within the government in the fall of 1993. The draft order reflected many of the concerns expressed by the critics. As of March, 1994, the new order had not been issued.[58]

Economically, the classification system may be too expensive for the decreasing budget of the 1990s. Reduced defense spending provides motivation for a less costly system. The costs of running the system, especially the storage of the hundreds of millions of pages of classified material, and the economic drag on industry and technology growth, could be prime targets of a budget cut.[59] The classification system, and the rest of the secrecy policies, if seen as unnecessarily big for the new national security environment, will be modified to meet a smaller mission, thereby reducing associated costs.

Any change to the classification system would require a redefinition of "damage to the national security" based on a new national security policy. A prevalent theme among the

people interviewed for this paper was that classification was appropriate to a smaller set of information, but that the system needed better protection for the information deemed sensitive. Since so much information is classified, people have trouble determining what information needs protection commensurate with the classification level and what information can be used for other purposes. This problem was well expressed by Justice Potter Stewart in the Pentagon Papers case.

> When everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion. I should suppose, in short, that the hallmark of a truly effective internal security system would be the maximum possible disclosure, recognizing that secrecy can best be preserved only when credibility is truly maintained.[60]

4.7 Suggested Improvements

Numerous proposals have been made on modifications to the classification system in order to reduce costs and improve public access to government information. These modifications claim to tighten the current definition to reduce the information which can be classified, eliminate some of the backlog of previously classified information, and strengthen administrative procedures.

4.7.1 Classification Regulation

For classification and its associated costs to be made manageable, the amount of information classified each year needs to be reduced below that declassified. Otherwise, the cost of storage of archival material will continue to increase, probably overriding savings in other areas. Many suggestions have been made on ways to reduce the amount of information classified. The classification definition could be modified to emphasize military and foreign policy and to deemphasize the nonmilitary information now included in the scope of classification. Some ambiguity could be eliminated by providing detailed guidance on what should be classified—presumably material closely related to military or foreign affairs—or by explicitly defining information that should not be classified.

An example of explicit guidance was suggested by Morton Halperin, who defined categories of information that would automatically be unclassified, categories that would be presumed classified, and information that would need to be individually reviewed.[61] Halperin

suggested that information about American forces in combat or in imminent danger of combat, American forces abroad, nuclear weapons abroad, and financing of foreign operations should be automatically unclassified. He recommended that weapon systems—details of advanced system design and operational characteristics—details of plans for military operations, details of diplomatic negotiations, and intelligence methods—codes, technology, and identity of spies—be classified.[62]

4.7.2 Declassification

Further declassification is also necessary to reduce the volume of classified material. The Defense Science Board Task Force on Secrecy, while saying that most technology should be unclassified, recommended that classified technology should be quickly declassified: "As a general guideline, one may set a period between one and five years for complete declassification."[63] According to Steven Garfinkel, Director of ISOO, millions of pages of information, classified for procedural reasons, could be declassified through small changes in current practices.[64] These procedural classifications occurred in cases where the government refused to acknowledge the existence of organizations, for example, its refusal to admit the existence of the National Reconnaissance Office (NRO)[65] even though that organization had been extensively discussed in the press and in books for twenty years. Every document on NRO letterhead was therefore classified, although often nothing other than the name merited it.

The ISOO recognizes that a large percentage of older material have lost their sensitivity, owing either to the passage of time or to changed national security circumstances.[66] Unfortunately, there is no way to determine accurately the small percentage of remaining sensitive materials without examining each document individually. With manual review is out of the question because of cost and resource limitations, mass declassification methods are necessary.

Three methods of mass declassification have been used in the past: automatic declassification, a drop-dead date, and sampling. Automatic declassification was used by executive orders. A drop-dead date automatically declassifies everything prior to the specified date, with exceptions for classes of information (such as intelligence sources) or for individual documents approved by senior officials. The date would need to be at least forty years to be

acceptable to the various executive agencies (and thus would allow declassification of all documents prior to 1953).[67] Sampling involves reviewing a small portion of the available documents to determine which can be declassified on the basis of the contents of the sampled portion. This method was used in the mid-1970s to declassify much of the Vietnam material. With proper safeguards, such as limitations on the number of exceptions,[68] any of these methods could reduce the amount of classified material, although at some minimal risk of releasing sensitive information.

4.7.3 Administration

A strong administrative commitment will be necessary to make any headway in the implementation of the classification system. Bureaucratic inertia, well insulated by the national security mindset, resists change in administrative practices. To have lasting effect, the administration, with congressional support, would need to change administrative procedures to encourage less classification. Proposed improvements include the following:

- Define real penalties for misuse of the classification system, either deliberate overclassification of information or use of classification for political purposes;

- Give the oversight organization additional power to review classification decisions and penalize misuse;

- Further reduce the number of people and organizations with original classification authority;

- Require additional training for original classifiers to ensure that they have the same understanding of the definition and that they use it uniformly;

- Make classifiers accountable by appraising their adherence to classification regulations during their performance review;

- Allow Congress to play a larger part in the definition of classification. Critics feel that a statute that would reflect the scope and broad guidelines of classification would have more affect on changing the intransigence of the bureaucracy than an executive order.[69]

Notes

1. Defense Science Board Task Force on Secrecy, 1.

2. Two books that give good descriptions of the underlying causes of classification and secrecy are Sissela Bok, *Secrets* (New York: Random House, 1983) and Edward A. Shils, *The Torment of Secrecy: The Background and Consequences of American Security Politics* (Carbondale and Edwardsville: Southern Illinois Univ., [1956] 1974).

3. E.O. 12356 47, Federal Registry 14874, April 6, 1982.

4. E. O. 12356, §2.1.

5. Derivative classification represented about 92 percent of the classification decisions in 1992. Information Security Oversight Office, 1992 Annual Report, 10-14.

6. Interview by the author with Michael Levin, Senior Classification Authority, NSA, Dec. 10, 1992.

7. E.O. 12356 §1.2(d)(1).

8. Ibid., §1.3(a).

9. Ibid., §1.1(a).

10. Ibid., §1.3(c).

11. Ibid., §1.4.

12. Ibid., §1.6.

13. William G. Phillips, "The Government's Classification System," in *None of Your Business: Government Secrecy in America*, edited by Norman Dorsen and Stephen Gillers (New York: Viking Press, 1974), 66. The Defense of Department's Coolidge Committee, November 1956 (H. Rept. 1884 June 21, 1958) reported that "The Committee has found a tendency on the part of Pentagon officials to 'play it safe' and overclassify; an abuse of security to classify administrative matters; attempts to classify the unclassifiable; confusion from basing security on shifting foreign policy; and a failure to declassify material which no longer needs a secrecy label." Ibid., 67: The Commission on Government Security (Wright Commission), June 1957, recommended, among other things, that the number of persons authorized to classify be reduced, the Confidential level be abolished because of overuse and its restriction upon the free flow of scientific and technical information, and the establishment of a Central Security Office to monitor the classification system.

14. E.O. 12065.

15. Anthony Lewis, Introduction, *None of Your Business: Government Secrecy in America*, 16.

16. Aftergood, "Secret Presidential Directives," 1.

17. Halperin and Hoffman, *Top Secret*, 36-40.

18. Snepp v. United States, 444 U.S. 507 (1980).

19. New York Times Co. v. United States, 403 U.S. 713 (1971).

20. See: Frederick Kaiser, "The Amount of Classified Information: Causes, Consequences, and Correctives of a Growing Concern," *Information Quarterly*, **6**, 3 (1989), 247-266; Defense Science Board, "Task Force on Secrecy," 1-5; and Phillips, "The Government's Classification System," 73.

21. Information Security Oversight Office, 1992 Annual Report, 17.

22. Interview by the author with Mike Levin, Senior Classification Authority, NSA, December 1992.

23. Samuel Fromartz, "Open Secrets," *Columbia Journalism Review*, March-April 1990, 34.

24. Charles G. Cogan, *The New American Intelligence: An Epiphany*, Project on the Changing Security Environment and American National Interests, Working Paper No. 3, (Cambridge, Mass.: Harvard University, January 1993), 8.

25. ISOO, 1992 Annual Report, 8. The ISOO reviews a small sample of classification decisions each year to determine how well the system is actually being implemented. The specific figures for 1992 are: Questionable overclassification, 1.7 percent, Clear-cut overclassification, 1.5 percent, Partial overclassification, 1.4 percent, Overgraded, 0.2 percent.

26. Espionage Act, Ch. 30, 40 Stat. 218.

27. E.O. 12356, §5.4.

28. Interview by the author with Steven Garfinkel, Director, ISOO, Jan. 28, 1993. A small number of employees, especially in DOE, have received informal sanctions. Source: Roger Heusser, Dept. Dir., Office of Declassification, DOE, phone conversation with author, March 4, 1994. Stephen Garfinkel remains source that these are very isolated cases.

29. Unpublished conclusion of Director of Central Intelligence (DCI) task force on classification; interview with Michael Levin.

30. Source: Roger Heusser, Dept. Dir., Office of Declassification, DOE, phone conversation with author, March 4, 1994.

31. 5 USC §552(6)(C)(b)(1)(A).

32. Interview with S. Garfinkel.

33. Kevin Galvin, "JFK Recordings Bound by Swirl of Red Tape," *Boston Globe*, Friday, Feb. 5, 1993, 20.

34. ISOO, 1992 Annual Report, *ii*.

35. ISOO, 1991 Annual Report, 19.

36. Steven Aftergood, "Garfinkel Speaks," 3. Question by S&GB: "But is it correct that more pages are being classified than declassified? Garfinkel: Yeah, I think so. But again the thing you have to understand is that classification decisions result in duplication. If we were to give the classification number in pages, people would immediately say, OK, the universe increased by that many pages this year. No it didn't! The universe increased by a lot more than that. It went out, it mushroomed."

37. E.O. 10964, §4(B)(a).

38. E.O. 12065 43 Federal Register 28949 (July 3, 1978).

39. Interview, S. Garfinkel.

40. Interview with M. Levin.

41. The Wright Commission, quoted in Phillips, "The Government's Classification System," 66; Senate Select Committee on Intelligence, "Meeting the Intelligence Challenge," 1985, quoted in Kaiser, "The Amount of Classified Information," 252.

42. ISOO, *1992 Annual Report*, 10.

43. Ibid.

44. Paul Quinn-Judge, "Pentagon hid weapons costs, GAO tells panel," *Boston Globe*, Friday, June 11, 1993, 3. A GAO investigation determined that the military gave GAO, an arm of Congress, deliberately false information or refused to provide information on some weapon system. In a report to the Senate Government Operations Committee, Eleanor Chelimsky, the GAO investigator said that the deception was deliberate. In an interview with the reporter, she supported her statement by saying "We have a memo that says 'these are the data that we have sent to GAO and these are the correct ones.'" Further, citing national security, "the military refused to hand over data on the reliability of the MX 'Peacekeeper' warhead" that they had previously furnished.

45. Rosamund M. Thomas, *Espionage and Secrecy: The Official Secrets Acts 1911-1989 of the United Kingdom* (N.Y.: Routledge, Chapman, and Hall, 1991), 215-216.

46. Ibid.

47. Interview with S. Garfinkel.

48. Aftergood, "The Perils of Government Secrecy," 81-88.

49. Defense Science Board Task Force on Secrecy, 1.

50. See U.S. Congress, Office of Technology Assessment, "Federal Scientific and Technical Information in an Electronic Age: Opportunities and Challenges," in Appendix B, Bureau of National Affairs, *Federal Information in the Electronic Age: Policy Issues for the 1990s* (October 1989), B25-B50, which provides an excellent discussion of the issue; National Academy of Sciences, *Scientific Communication and National Security* (Washington D.C.: National Academy Press, 1982); and *Striking a Balance: National Security and Scientific Freedom First Discussions*.

51. Defense Science Board, "Task Force on Secrecy," 1-2, 9.

52. Cox, *Myths of National Security*, 2. In 1973, pollster Louis Harris conducted a study entitled "Confidence and Concern: Citizens View American Government" for the Senate subcommittee on Intergovernmental Relations. The survey concluded among other things that "government secrecy no longer can be excused as an operational necessity, since it can exclude the participation of the people in their own government, and, indeed can be used as a screen for subverting their freedom" (Cox, 2).

53. Halperin and Hoffman, *Top Secret*, 1.

54. Representative Henry Gonzales, Letter to the Editor, *Issues in Science and Technology*, Fall 1992, 7.

55. Interview with S. Garfinkel, who claims that ISOO review has not detected any cases of abuse of the classification system by government officials trying to hide politically embarrassing actions. He says that their sampling techniques would detect any widespread political abuse of this type.

56. Robert Gates, "Statement on Change in CIA and the Intelligence Community," April 1, 1992.

57. Britt Snider, General Counsel to the Senate Intelligence Committee, interview with the author, April 1993.

58. John Aloysius Farrel, "White House orders secrecy policy review," *Boston Globe*, Wednesday, May 26, 1993, 3.

59. ISOO, 1992 Annual Report, 2; on the benefits of a declassification program, the Southeast Asia Project [not clear: whose?]: "FOIA requests and inquiries from researchers are far less time consuming than before and far more productive. Also, with millions fewer classified pages, storage and protection costs are far lower."

60. United States v. New York Times, 403 U.S. 713, 729 (1971) (concurring opinion by Justice Stewart), quoted in Halperin and Hoffman, *Top Secret*, 85.

61. Although Halperin's suggestions were made (in writing) during the 1970s, critics of classification in the 1990s still support his basic idea. Aftergood, "The Perils of Government Secrecy," 86-87.

62. Halperin and Hoffman, *Top Secret*, 57.

63. Defense Science Board Task Force on Secrecy, 2.

64. Interview with S. Garfinkel.

65. Aftergood, "NRO Declassified," *Secrecy & Government Bulletin*, 15 (October 1992), 1.

66. Interview with S. Garfinkel.

67. Ibid.

68. Aftergood, "Special Issue: Automatic Declassification," *Secrecy & Government Bulletin*, 17 (December 1992), 1.

69. Kaiser, "The Amount of Classified Information," 261.

Chapter Five

Export Control

> The acquisition of national security sensitive goods and technology by the Soviet Union and other countries the actions or policies of which run counter to the national security interests of the United States, has led to the significant enhancement of Soviet bloc military-industrial capabilities.
>
> Export Administration Act[1]

5.1 Export Control History

Secrecy encompasses more than classification. The Cold War was believed to require controls on the free movement of unclassified information and technology out of the United States. In theory, these controls prevented an adversarial government from using U.S. technology, either as information or embedded in a product, to gain a national security advantage. Policy questions related to the broad category of technology transfer are discussed in this and the following two chapters. This chapter deals with the export control restrictions placed on the movement of embedded technology, whether government, industrial, or academic. **Chapter Six** looks at limitations on commercializing military restricted technologies, and **Chapter Seven** at mechanisms that protect technology information.

In an attempt to adapt to the post-Cold War situation, the export control system[2] recently redefined its objectives and fundamental strategy. With the system seen by many critics as a relic with decreasing national security relevance and as hampering U.S. competitiveness,[3] since 1990 its controlled items have been reduced by two-thirds[4] and 70 percent of export license applications were eliminated.[5]Yet, even though dramatic steps have been taken to adjust to post-Cold War realities, the countervailing trends of increasing economic globalization may further reduce the viability of export controls as a national security option.

5.1.1 Economic Sanctions

Export restrictions, in the form of economic sanctions, have been used for foreign policy purposes. Between 1914 and 1984, the U.S., either unilaterally or in conjunction with allies, applied peace-time sanctions sixty-one times[6] and between 1985–89 another twelve times.[7] Examples of sanctions applied in 1993 include Serbia, Cuba, and South Africa. Among

rationales for economic sanctions have been human rights, punishment for anti-American actions, noncompliance with international treaties (especially nuclear nonproliferation), strategic deterrence from possible future aggression, and as a prod for action desired by the U.S.[8]

Foreign policy sanctions often provide a symbolic indication of the intent of the U.S. government and apply direct pressure on an another government without recourse to military action. Their symbolic nature means that their success or failure should be judged by their political ramifications rather than national security impacts. Other problems include the difficulty of balancing the competing objectives of sanctions and national security controls with the cost compared with that of other political gestures, heightened tensions between the U.S. and other governments owing to unilateral sanctions, and the diffuse nature of most such sanctions which makes them difficult to enforce and undermines their effectiveness.[9] Although foreign policy controls are an important topic, the remainder of this chapter focuses on national security controls.

5.1.2 National Security Controls

Export controls have been used by the U.S. for national security purposes[10] throughout its history but were institutionalized with the passage of the Export Control Act of 1949 and the introduction that year of the Coordination Committee on Multilateral Export Controls (COCOM).[11] As of May 1993, COCOM consisted of all NATO countries plus Iceland, Japan and Australia. Additional legislation froze the Cold War objectives of export control into statutes, limiting the ability of the U.S. to implement new export control objectives. Major statutes[12] that cover export control include the Mutual Security Act of 1954, which includes the International Traffic in Arms Regulations (ITAR), the Export Administration Act of 1985 (EAA85),[13] implemented by the Export Administration Regulations (EAR), and the Arms Export Control Act of 1976. Three separate export control lists are used: the Commodity Control List (CCL), which contains dual-use products; the Munitions Critical Technologies List (MCTL), which contains military products; and the Atomic Energy List, which contains nuclear products. The EAA expired in 1990, and although an extension was vetoed by President Bush[14] the provisions were extended by executive order[15] while the Congress and the president worked on a fundamental reform of export control. As of June

1993, Congress had not yet passed a modification of the EAA. The following provides an example of the continuing Cold-War mentality:

> It is the policy of the United States, particularly in light of the Soviet massacre of innocent men, women, and children aboard Korean Air Lines Flight 7, to continue to object to exceptions to the International Control List for the Union of Soviet Socialist Republics.[16]

Another example is the explicit requirement to consider whether a country is still communist when determining which controls may apply to it.[17] Legislation that attempts a fundamental change in U.S. export control regulations is currently pending in Congress.[18] **Table 5-1** gives a synopsis of the history of export control.

Export control regulations were not static but changed throughout the Cold War to reflect shifts in the U.S.-Soviet relationship. Controls in the 1950s were very tough and included a near-total ban on commerce with the communist bloc. Gradual loosening of the controls in the 1960s and 1970s were reflected in a liberalized Export Control Act of 1969 which limited controls to only national security products and technology.[19] During these years the importance of export controls as an instrument of policy lessened, and COCOM faded in importance.[20] The Bucy Report,[21] a critical review in 1976 by the Defense Science Board of the export control assumptions, called for a redirection of the focus of controls from embedded product technology to design and manufacture know-how. Its recommendations were adopted in the 1979 amendment to the EAA.[22] After President Reagan took office, COCOM was revitalized as an instrument of political pressure against the Soviet Union,[23] and in the first high-level meeting of COCOM principals in twenty years, the controls were tightened. Reagan also aggressively targeted dual-use technology, going beyond the EAA to control not only military but also commercial technology. The types of technology denied to the Soviets through export controls are shown in **Table 5-2**.

5.1.3 Post-Cold War Export Control

The collapse of the Soviet Union achieved the primary U.S. national security objective of the controls. Politically, the pressure against further export controls by industry became stronger. The U.S. substantially reduced and modified its export control regime to reflect the new political realities and attempted to broaden the controls to encompass previously secondary threats, for example, proliferation of weapons of mass destruction and terrorism.

Table 5-1

Export Control History

Year	Technology and Control Measures
1940	Early export controls during World War II.
1949	Export Control Act requires examination of exports to the Soviet bloc. Department of Commerce administers the act by means of Export Administration Regulations. Commodity Control List developed. Coordinating Committee for National Export Control (COCOM) organized, Three lists of controlled items maintained.
1954	Mutual Security Act includes International Traffic in Arms Regulations regarding export of military items.
1969	Export Administration Act of 1969 reflects detente by encouraging trade with all countries.
1976	Arms Control Act.
1979	Export Administration Act of 1979 changes the focus from goods to technology, thus reflecting the Bucy report. Military-critical technology's list (MCTL) created.
1981	Reagan administration views the criticality of technology transfer occurring in scientific exchanges. All validated export licenses with the USSR are suspended. At the first high-level meeting of COCOM in twenty years the administration requests cooperation from allies in restricting technology transfer. National Security Council Technology Transfer Coordinating Committee established by the Director of Central Intelligence.
1982	National Academy of Science Panel on Scientific Communication and National Security, commonly called the Corson Committee, completes report that recommends criteria for restrictions on university-related research.
1983	Export Administration Act of 1979 expires amidst heightened controversies over tightening or loosening controls on technology transfer. Administration continues regulatory mechanisms by executive order followed by a temporary extension of the Act by Congress. U.S. and Japan sign agreement on the exchange of defense technologies. U.S. liberalizes export control policy toward China.
1985	Export Administration Act of 1985.
1988	Omnibus Trade and Competitiveness Act modified and extended the Export Administration Act. In response to the Toshiba–Kongsberg incident (see Chapter Five), the bill added the Multilateral Export Control Enhancement Amendments Act (MECEAA), which increased the penalties against companies that violate export control regulations.

Table 5-1 continued

Year	Technology and Control Measures
1990	Strategic Review of Export Control Regime by President Bush. Expiration of the Export Administration Act of 1985. The president pocket vetoes its replacement. COCOM agrees to 33 percent reduction in the control list. The president introduces the Enhanced Proliferation Control Initiative (EPCI) to combat the proliferation of weapons of mass destruction.
1991	New reductions in COCOM control list in response to dissolution of the Soviet Union.
1992	Introduction of the Cooperation Forum to include the former Warsaw Pact countries. The Forum seeks to extend nonproliferation controls to the former Soviet Union and its allies in exchange for further reductions of export controls. U.S. eased licensing requirements on exports to COCOM countries.

Source: adapted from Table A, Anthony T. Green, *U.S.–Japan Technology Transfer: Accommodating Different Interests* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, 1986, P-86-1).

In January 1990, President Bush announced a strategic review of the export control system in response to the initial separation of the Warsaw-Pact countries from the Soviet Union. Two major questions were raised, centered on how to help the economies of the emerging eastern European countries without helping the Soviet military and on the need, achievability, and appropriateness of changing the focus of export control to inhibit proliferation of weapons of mass destruction.[24] The review resulted in May 1990 in important changes in U.S. policy. The U.S. would support scrapping of the old control list with the development of a new "core" one. The review identified forty-three out of 120 technologies that could be completely or partially decontrolled and recommended examining priority technologies—computers, telecommunications equipment, machine tools—for immediate partial decontrol. It also recommended easing controls on eastern European countries that adopted safeguards approved by COCOM.[25]

In June 1990, COCOM agreed to a 33 percent reduction in existing export control regulations.[26] The COCOM countries agreed to establish a core list of eight technologies that needed continuing controls, including telecommunications and computers, electronics design, development and production, and advanced materials.[27] COCOM agreed to the U.S.

Table 5-2

Potential Gains for Soviet Bloc in the Absence of U.S. Controls

Automated Production and Control Technology

- Significant impact on strategic weapons systems production (e.g., strategic aircraft, submarines, etc.)
- Very large Soviet defense budget savings

Telecommunications Technology

- Assist in improved [Warsaw] Pact networking (C^3I)
- Improved telecommunications R&D instruments—important for robust systems for the future
- Supporting technology for EW R&D in at least three distinct areas

Miceo Electronics/Semiconductor Technology

- Significant assistance for military IC production (particularly for faster production or more complex parts)
- Cases showed large potential impact for systems with high production quantity (e.g., air-to-air missiles

Computer technology

- Support of Soviet 32-bit supermini-computer R&D
- Compact computer and Winchester disc technology for the [Soviet] Bloc

Sensor Technology

- Signal processing technology directly applicable to key military systems (e.g., ASW sensors, radars)
- Lithium niobate materials for military acoustic wave devices

Electro-optics and Optoelectronics Technology

- Support for fiber optics and optoelectronics R&D

Power Generation/Propulsion Technology

- Solid propellant R&D
- High quality bearing production capability with potential for enhancement of aircraft engine reliability as well as for other military platforms

Genetic Engineering

- Research instrumentation for probable use in Soviet BW/CW R&D

Transportation Technology

- Enhanced aircraft computer-aided design and manufacturing capability

ASW = antisubmarine warfare
BW/CW = biological/chemical warfare
EW = electronic warfare
IC = integrated circuit

Source: Office of the Undersecretary of Defense for Policy, *Assessing the Effect of Technology Transfer on U.S./Western Security: A Defensive Perspective* (Washington, D.C.: February 1985), Figure 4-2.

recommendations on easing controls on the East European countries and on partial decontrol of the high-priority technologies.[28]

President Bush also broadened the export control mission to include nonproliferation. COCOM controls, aimed primarily at the Soviet bloc, did not cover exports to some countries that were trying to acquire weapons of mass destruction.[29] On November 16, 1990, E.O. 12735, which dealt with the threat of chemical and biological proliferation, was issued. Citing his "deep concern about the serious threat posed by chemical and biological weapons," Bush declared a national emergency and invoked the International Emergency Economic Powers Act.[30] On December 13, 1990, the administration announced the Enhanced Proliferation Control Initiative (EPCI) to combat the spread of missile technology and nuclear, chemical, and biological weapons. The EPCI expanded export controls for technology used in the manufacture of chemical, biological or missile weapons, such as chemical precursors, or equipment used in manufacturing these precursors.[31]

In response to continuing changes in the former Soviet Union, export control needs similarly to be modified. In August 1991, COCOM reduced the number of products subject to export control rules by another 50 percent,[32] bringing the total reduction since 1990 to 66 percent. In April 1992, the Department of Commerce announced new licensing regulations that eased requirements on controlled exports to COCOM countries, countries cooperating with COCOM controls, and reexport licensing requirements. These regulations expanded eligibility for general licenses to additional technologies, including roughly 95 percent of all items restricted by national security.[33] Among the items excluded from the new regulations were supercomputers and cryptographic equipment. The rules also eliminated reexport restrictions on U.S.-controlled items except for reexport to countries on the nonproliferation list and on items excluded from general licenses. The Commerce Department estimated that these rules would immediately deregulate $2–3 billion a year in exports.[34] In June 1992, East-West export controls were further liberalized with the agreement to start a Cooperation Forum on Export Control between the COCOM nations and the former members of the Warsaw Pact to discuss the development of COCOM-like rules for the East European countries in order to deter proliferation of technology for weapons of mass destruction. In return, COCOM offered the incentive of further relaxation of export controls to countries instituting an export control regime.[35]

5.2 Export Control Assumptions

In spite of substantial liberalization of export control rules, the export control policy still has many critics. Among the most common criticism of the system are that regulations are too complicated, too much technology remains controlled, the security objectives do not properly reflect today's environment, the policy does not reflect trends in modern technology, and enough consideration is not given to economic factors. Such criticism must be addressed in adapting export control to the post-Cold War era.

Although such political considerations as the relationship between the U.S. and the former Soviet Union dominate export control discussions, other issues, such as changes in technology, also need attention. Since 1949, changes in both the technological and the political environment may have diminished the ability of export controls to accomplish their objectives. For effectiveness, export controls rely on some fundamental assumptions about technology and its movement around the world, among them the following, which were true in the 1940s:

- the U.S. is the leader in, and controls the diffusion of, most advanced technology;
- exports do not much matter to the U.S. economy, so commercial costs are small;
- dual-use technologies represent a relatively small and easily isolated category of exports[36]; and
- technology has a long life cycle and evolves slowly enough so that obsolete technology is not useful to an adversary.

In a study in 1991 the National Academy of Sciences (NAS) noted that these assumptions are no longer valid, and it identified current trends that affect export control:

- the increasingly rapid global diffusion of technology;
- declining eminence of U.S. technology and manufacturing;
- the growing importance of exports to the economic vitality of the U.S.;
- rapid technological progress, leading to the extension and "filling in" of the technological spectrum; and
- commoditization of many products, typified by low and steadily decreasing prices, high production volumes, a multiplicity of producers, and high degrees of substitutability of increasingly more powerful computer equipment.[37]

These trends change the way the U.S. will have to view export control and raise questions about the ability to protect truly important national security technology and the true economic impact of those protection mechanisms. Cutting-edge technology is not being produced only in the U.S. but globally. Advanced technology, with national security implications, has been reduced to a commodity, cheap and available from many sources. The U.S. cannot unilaterally make the economic rules, but must cooperate with the rest of the world. In the global economy, the cost of export controls cannot be ignored because the U.S. needs the economic benefits of exports. In 1991, this country exported a total of $421.9 billion.[38] In 1990, before liberalization, controls applied to 40 percent of U.S. manufactured exports, for a total of $120 billion.[39] Commercial technology turns over in time spans as short as a couple of years: it does not take long to go from state-of-the-art to obsolete and widely available. Some obsolete technology, especially computers, can still be useful to an adversary. But inclusion of obsolete technology on export control lists complicates enforcement, reinforces the notion that the lists were too large, and reduces the effectiveness of export controls.[40]

5.3 Policy Issues

Developing an export control regime that takes into account all the political, economic, and technical trends presents a daunting task. Numerous policy issues need to be examined and various tradeoffs between them must be examined. The basic question that needs to be decided is whether export control still fulfills an essential national security mission. If such controls remain necessary, what technologies must be protected and where and how can the line be drawn between sensitive technologies that need to be protected and technologies that need no control or else cannot be controlled. Specifically, what mission can export control accomplish? how should the technology subject to controls be identified? what is the definition of sensitive? what mechanism for administering the controls is appropriate? how to respond to the valid arguments against controls? and what are the implications of not being able to control technology?

5.3.1 Multiple Objectives

The multiple export control objectives, East-West controls and nonproliferation, have not, as of June 1993, been combined, and whether they can be easily is not clear. Export controls were used during the Cold War to prevent or delay the acquisition of sensitive technology by the Soviet Union and by the military of the Soviet Union and its allies (although hurting the

Soviet commercial economy was not an objective).[41] The continuing presence of COCOM regulations shows that controlling technology to the former Soviet military remains an objective. While the U.S. supports Russia's conversion to a market economy, as well as that of the other former Warsaw Pact countries, Russia is still a military superpower, and a hardline alternative to the current government with a military resurgence is not out of the question. Until Russia and the other former Soviet republics firmly establish stable democratic governments, the U.S. has a national security interest in helping their commercial economy while keeping advanced technology from the their military. This interest requires some form of East-West export control regime, although its practicality may be problematic.

Nonproliferation cannot be cast in the East-West ideological battles of the Cold War. Both the COCOM nations and the former Warsaw Pact nations have a common interest in ensuring that weapons of mass destruction do not proliferate. Because the former Warsaw Pact countries have technology useful to others developing weapons of mass destruction, these countries must be included in any effective export control regime. The Cooperation Forum encouraged nonproliferation controls in the former Warsaw Pact countries by basing the easing of East-West controls on the successful development of nonproliferation controls.

East-West and nonproliferation controls, however, may be mutually inconsistent. Gaining sufficient cooperation for a strong nonproliferation regime might be impossible while East-West export controls remain in place on Russia, because accepting restrictions might be against Russia's self-interest. Any export control policy will need to balance the need for both East-West and nonproliferation controls, and the required strength of each control regime, against the difficulty of meeting the individual objectives of either type of control.[42]

5.3.2 Information vs. Technology

Export controls have been applied very broadly, initially as technology restrictions but evolving to include restrictions on information flow.[43] EAR or ITAR controls apply to information used in the design, production, manufacture, use or reconstruction of materials on the Commodity Control List. The controls regulate transmission of the information from the U.S. and release of the information within the U.S. intended for foreign transmission. Controlled transmission includes visual inspection, oral exchanges in the U.S. or abroad, or

application abroad of information that originated in the U.S. General Licenses are provided for educational or scientific information.[44]

The long-term applicability of information restrictions is questionable in light of new export control missions. U.S. support for modernizing the Russian commercial economy requires Russian access to state-of-the-art dual-use information and manufacturing processes, much of which cannot be shared under a strict interpretation of the existing restrictions. Also, the evolving objectives alter the sensitivity of technological information. Managing nonproliferation, for example, depends less on information restrictions than on controlling the acquisition of raw material and manufacturing equipment. The knowledge needed to build weapons of mass destruction is so widespread that it lies outside any possible control system, as can be seen from periodic reports of students designing nuclear bombs from library books.[45] Export control must focus on the potentially controllable raw materials such as plutonium or chemical precursors. The countries at which nonproliferation controls are aimed do not possess the manufacturing capabilities to convert technological knowledge into weapons easily. Additional information, available through the relaxation of controls, will have little impact on the ability of nonproliferation controls to meet their objective. Another problem with information restrictions is that reduction in the free flow of scientific communications within the U.S.[46] negatively impacts the development of technology (see **Chapter Eight** for a discussion of this subject in greater detail).

5.3.3 New Definition of "Sensitive"

New missions may require new definitions of sensitive technologies and proscribed countries. Sensitive technology depends on the combination of mission and specific country. For example, sophisticated computer technology was important to the Soviet Union during the Cold War but may not be useful to an underdeveloped country developing chemical weapons. An underdeveloped country lacks the infrastructure to use computers to manufacture advanced weaponry but can build weapons using unsophisticated chemicals. What criteria will be used to place countries on the proscribed list? In the EAA the criteria for placing countries on the proscribed list included having a communist government, nuclear capabilities, sponsoring international terrorism, and conducting aggressive actions against the U.S. and its allies.[47] These criteria were sufficient to cover the main threats—the communist countries and "outlaw" governments such as Libya and Iran. In the 1990s, such simple criteria may be

insufficient. Additional criteria might need to be considered, such as the potential for reexporting technology to countries on the proscribed list (e.g., the Muslim countries of the former Soviet Union, which may evade controls against Iran or Iraq) or the stability of the region.

Defining new criteria is complicated, because the responsibilities for export control are scattered and decentralized in the U.S. government. The departments of Defense, State, Commerce, Treasury, and the Trade Representative all provide input into export control policy. Given the different missions of these organizations, disputes over the purpose and scope of export control are not surprising. These disputes result in "unclear and sometimes conflicting policies, long delays in reaching closure, uncertain lines of authority."[48] Although a centralized authority might reduce some organizational impediments, a central authority might be captured by one of the departments and policy skewed because the balancing arguments of the others might be ignored.

5.3.4 Regulations

Much criticism of U.S. export controls centered on the administration of the regulations, as shown by the following sample:

- the fundamental goals of export control were incorrect
- technology was often placed on the control list inappropriately and then inappropriately decontrolled
- U.S. controls were unilateral
- the licensing process was cumbersome
- penalties for violators need to be made more effective
- consultation needed with industry in order to balance economic and national security interests
- better enforcement of the foreign availability provisions[49] of the EAA needed.

(*i*) COCOM-based export controls depend on the prohibition of selected products from export to proscribed countries. An alternative approach, recommended in 1991 by the NAS study,[50] is to replace prohibition-based export controls with a control regime based on

incentives and end-use controls, analogous to intra-COCOM trade. With few exceptions,[51] COCOM countries allow free trade of technology within the COCOM community, because the countries have standard controls. End-use restrictions allow the U.S. to specify conditions on the use of the technology, such as location or availability of spare parts, which theoretically ensures that it cannot be reexported or misused. The U.S. permits unhindered movement of approved technologies through bilateral agreements (§5[k])[52] with countries that abide by specified end-use restrictions and reexport controls.[53] Initiation of incentive-based controls is one of the aims of the Cooperation Forum with East Europe and the former Soviet republics. Economically, incentive-based controls are likely to generate a larger export market than prohibition-based ones; the downside is that technology will be exposed to a larger audience and export controls unavoidably weakened as the number of countries participating increases.

(*ii*) Successful implementation hinges on placing the important and controllable products on the control lists. The present structure for determining the contents of the lists is haphazard. The 1991 NAS study found that

> The system of U.S. list management suffers from a lack of clear definitions and criteria for control and decontrol, as well as the widely varying formats and structures that exist for domestic and international lists. The fact that an item is taken off the Military Critical Technologies List, for example, does not necessarily lead to U.S. action to delete it from the COCOM or U.S. control lists.[54]

COCOM is particularly cumbersome, because changes, either to place technology on the list or to remove it, require unanimous agreement,[55] allowing any country unilaterally to block the control or decontrol of technology. This veto power leads to predictable accusations that the contents of the control lists are manipulated by their respective governments to further the country's commercial industry.[56] Historically, COCOM's desire to avoid a risk of exploitation caused retention of technology on the lists longer than necessary. As economic pressures to shorten the lists mount and the selection criteria become more abstract, the problem of not placing critical national security technology on the lists increases.

(*iii*) Because the national security and foreign policy objectives of the U.S. are different from those of its allies, multinational export control regimes may not always adequately address all the U.S. concerns. In this case, the U.S. can impose additional unilateral controls

and reexport requirements or accept the multinational controls, even though these do not provide the protection the U.S. believes necessary. The U.S. has often chosen to impose unilateral controls, but unilateral and extraterritorial controls damage allied relations and harm U.S. exporters. The NAS study concluded that

> Most foreign countries do not accept that the United States has jurisdiction over the actions of non-U.S. citizens outside the territory of the United States, and they view assertions of this jurisdiction as clear violations of international law. Moreover, data from the Department of Commerce suggests that in fact compliance with U.S. reexport control requirements by foreign citizens is exceedingly poor. . . . Reexport controls typically present thorny legal issues, are ineffective, and have a corrosive effect on the Western alliance.[57]

The problem of U.S. extraterritorial claims has dissipated somewhat, because West-West reexport requirements have been relaxed and are in place for only a few items. The possibility of reexport controls remains important in the context of possible East-West and nonproliferation missions. Given the trend in the former Soviet republics of selling military equipment and materials, preventing reexport of technology provided to the former Soviet republics under the Cooperation Forum may be critical.[58] Balancing the diplomatic and economic losses caused by a generally ineffective mechanism of reexport control against potential national security damage from uncontrolled reexport, especially in regard to nonproliferation, will be an important part of future export control policy.

(*iv*) Export control regulations are extremely complex and hard to understand, let alone comply with. The EAR, although approximately 550 pages long, does not encompass all the export control regulations. In addition to the CCL regulated by the EAR, there are eight other unclassified lists regulated by other departments, including the munitions and atomic energy lists, as well as the classified Military Critical Technologies List. The CCL alone is over 150 pages long and contains multiple control systems, including COCOM, missile technology, nuclear nonproliferation, and chemical and biological.[59]

The complexity of export control regulations entails a substantial cost for exporters, even those attempting to abide by the law, wanting to understand the regulations well enough to comply. Large firms have legal departments to ensure compliance, but small exporters, without adequate legal support, can very easily unintentionally violate the regulations. The 1987 NAS study found that:

> The complexity of U.S. national security export controls discourages compliance, especially by foreign firms and small-to-medium-sized U.S. companies. . . . [The EAR] could be reduced and simplified substantially-and made more "user friendly."[60]

Reducing the complexity lessens the government's ability to enforce the controls. A vague description eases evasion of the regulations because of the difficulty of consistently applying general rules to specific instances. A proper balance is necessary between overwhelming exporters with the rules and causing numerous unintentional violations, and defining loose rules that cannot be enforced against willful violators.

(*v*) Regulations that are understandable are not by themselves enough to ensure compliance. The government must also impose strong penalties on violators. Current penalties for export control violations defined in the EAR include fines up to $1 million for national security violations and civil penalties up to $100,000, the ability to suspend or revoke an individual's or company's privilege to export, or the seizure of goods being improperly exported.[61]

Recent history shows that these penalties may not be sufficient to discourage purposeful violations.[62] An example is the mid-1980s case in which Toshiba and Kongsberg were accused of selling machine tools to the Soviet Union in excess of the capabilities allowed by the control lists.[63] Investigation disclosed that this diversion was not an isolated incident, but that other companies, including French, Italian, West German, and British companies, had also sold illegal machine tools to the Soviet Union,[64] which used the acquired technology to build quieter submarines, thereby reducing an important military advantage of the U.S.[65] The U.S. had limited options, because the technology transfer occurred outside the U.S. and did not involve U.S. technology. It had no legal jurisdiction over the companies, because the violation was against Japanese export control laws. As punishment, the U.S. for the first time applied import sanctions by imposing a three-year ban on U.S. imports from Toshiba and a bar on government contracts for the company.[66]

The economic impact of unilateral sanctions is inversely proportional to their damage to the U.S. economy. Foreign companies with a large U.S. presence will be greatly affected, but so will their U.S. customers, while companies with no U.S. presence will not be hurt.[67] Under pressure from U.S. firms dependent on Toshiba technology, the U.S. reduced the

penalty to alleviate harm to U.S. companies. Consequences of unilateral sanctions may affect the relationship between the U.S. government and the government of the offending company and may increase pressure on that government to enforce the regulations. The penalties for violating them should be strong enough to discourage purposeful violations, applicable to all violators uniformly, should not penalize innocent companies whose own survival depends on that of the company in violation, and should minimize diplomatic consequences. They should also distinguish by severity between innocent companies that violate the law out of ignorance and purposeful violators.

5.3.5 Industry Participation

For export control to work, industry must accept the needs and adequacy of the regulations. Without industry support, a company interested only in profits could use many loopholes to bypass the regulations. Historically, the government did not consult with industry during development of the controls, and as a result economic national security concerns were not properly balanced.[68] According to Ronnie L. Goldberg, member of the U.S. Council for International Business, industry is increasingly consulted on export control policy.[69] National security and economic considerations, however, do not always coincide. Because export controls support a national security objective, trying too hard to get industry, which has an economic objective, to understand and cooperate might blur the national security focus. The policy needs to balance the operational efficiency gained through industrial cooperation against the possible weakening of national security.

5.3.6 Foreign Availability

The Export Administration Act, Section (f), states:

> The Secretary. . .shall review, on a continuing basis, the availability to controlled countries, from sources outside the United States, including countries which participate with the United States in multilateral export controls, of any goods or technology the export of which requires a validated license. . .the Secretary determines. . .that any such goods or technology are available in fact to controlled countries from such sources in sufficient quantity and of comparable quality. . .the Secretary may not, after the determination is made, require a validate license.[70]

Although the intent of the provision, that freely available technology should not be controlled, is clear, the provision has not resulted in timely decontrol of available technology.[71]

Restrictions on U.S. exports of commonly available technology impose an economic burden on U.S. companies without increasing national security.

Foreign availability is but one instance in which export controls have not responded to trends in global technology. High technology has been diffused worldwide through joint ventures, technology licensing, scientific communication, sale of equipment, among other methods. Most technology critical to national security can be derived from what is widely available from non-COCOM countries that have minimal export controls. Even if all the countries that possess proscribed technologies were to abide by an export control regime, the sheer number of countries necessary for effective control defeats the purpose. The ubiquity of much high technology today, such as computers, along with the ease of technical diffusion prevents effective control on most technology. Export control policy must accept that some technology that should be controlled for national security reasons is beyond its reach. The policy must determine the technologies that can be physically controlled and what measures effectively used to protect them.

5.4 Costs and Benefits

Identification of the relative costs and benefits of export control has been a longstanding question. Advocates can point to studies that demonstrate both enormous commercial costs and equally large government savings. Economic arguments will be very important in the debate over the appropriate scope of post-Cold War controls. The national security objectives supported by the controls will need to be balanced by their economic cost. Cost and benefit analyses were published by both the DOD and the NAS in the mid-1980s.[72] Although changes in the export control system in 1991-93 make the specific historical costs and benefits unimportant to the current debate, the methodologies used to gauge them can be applied.

When the NAS looked at the cost of export control in 1987, it estimated an overall commercial cost for 1985 of $9.3 billion,[73] an estimate that since then has been extensively quoted by advocates of looser controls.[74] The numbers[75] should be regarded, however, as only very rough approximations, because many of the underlying numbers were very soft. Yet the NAS study does provide a framework within which to examine factors that contribute to the cost which can be studied to determine the impact of changes on that cost. The study

defined several categories, shown in **Table 5-3**, including direct expenditures and indirect costs, with negative economic impacts.

Table 5-3

Factors Affecting Costs of Export Control

- Direct administrative costs
- Indirect administration costs
- Lost West–West export sales
- Lost West–East export sales
- Lost sales by U.S. firms of components incorporated into foreign products
- Lost sales because of foreign policy controls
- Reduced spending on R&D
- Indirect R&D impacts (e.g., technical data restraints, control of foreign scientists in U.S. industrial labs)
- Uncertainties in license procedures
- Effect of discouragement on small businesses in West-West trade owing to complexity of license procedures (i.e., they forego attempting to export)
- Warehousing and other costs incurred when available products must await a license
- Lost profits from denied or delayed export and foreign sales
- Long-term influence of U.S. controls on relationship between U.S. and foreign customers (qualitative evidence suggests in some cases U.S. firms are least preferred suppliers, all else being equal)

Source: Adaptation of National Academy of Sciences, *Balancing the National Interest: U.S. National Security Export Controls and Global Economic Competition* (Washington, D.C.: NAS Press, 1987), Table D-1, 256, combined with Table D-3, 266.

In 1985, the DOD published an analysis of national security benefits achieved by the U.S. through export control that examined the savings the Soviets would accrue from gaining access to U.S. technology and the extra defense costs needed by the U.S. to offset those gains. The study concluded that it would cost the DOD an additional $20–$50 billion a year in increased R&D and procurement to maintain its position relative to the Soviet Union if all export controls licenses in 1983–84 were approved.[76] This report, like the NAS study of costs, was used extensively in the public debate over export control and was the underpinning for a movement favoring more stringent controls.[77] The methodology, additional R&D and procurement costs of new defense systems, used to determine the costs, was the same one

used by the Omnibus Trade and Competitiveness Act to determine penalties against violators of export controls.[78] As in the case of the NAS study, while the methodology is interesting, the figures are suspect.[79] For example, the DOD study does not include six of the military critical technologies known to be targeted by the Soviets; the Soviets realize almost all their savings ($6–$12 billion out of a total of $6.695-$13.26 billion) from the acquisition of just one technology—automated production and control machines— but it used constant 1985 dollars to calculate costs through 1997.[80] As was true of the costs, no reliable figures are available for export control benefits.

Notes

1. 50 USC §2401(11).

2. Three good studies of the basic policy considerations for export control are: Committee to Study International Developments in Computer Science and Technology, *Global Trends in Computer Technology and Their Impact on Export Control* (Washington, D.C.: National Academy Press, 1988); National Academy of Sciences, *Balancing the National Interest: U.S. National Security Export Controls and Global Economic Competition* (Washington, D.C.: national Academy Press, 1987); and its follow-up study Panel on the Future Design and Implementation of U.S. National Security Export Controls, *Finding Common Ground: U.S. Export Controls in a Changed Global Environment* (Washington, D.C.: National Academy Press, 1991). These related studies trace export control policies at the end of the Cold War and the beginning of the post-Cold War period.

3. Cf. Robert Kuttner, "How 'National Security' Hurts National Competitiveness," *Harvard Business Review*, Jan.-Feb. 1991, 140.

4. Interview by the author with George Menas, Director, Strategic Policy, Defense Technology Security Agency, Jan. 27, 1993.

5. Computerram International, "Soviet Focus; RISCs still banned, seem to be the one anomaly in the new liberal COCOM export rules," Apt Data Service (U.K.), August 14, 1991.

6. Gary Clyde Hufbauer and Jeffrey J. Schott, "Economic Sanctions: An Often Used and Occasionally Effective Tool of Foreign Policy," in *Export Controls*, edited by Michael R. Czinkota, Table 2-1, 18.

7. Richard Ellings, "The End of Economic Sanctions?" in *Private Property and National Security Foreign Economic Sanctions and the Constitution*, edited by Richard J. Ellings et al. (Washington, D.C.: National Legal Center for Public Interest, 1991), 21.

8. Gary Clyde Hufbauer, Jeffrey J. Schott, and Kimberly Ann Elliot, *Economic Sanctions Reconsidered*, Vol. 1 (Washington D.C.: Institute for International Economics, 2nd ed., 1990), Table 3.2 through 3.5, 59-61, and Table 5.1, 93. The authors concluded that the effectiveness of controls varied with the objective. The controls were generally effective when used for destabilization, somewhat effective for modest policy goals, and not effective when used to disrupt military potential or in seeking large changes in another country's policies. Richard Ellings, in "The End of Economic Sanctions?" (p. 23), however, reports that the effectiveness was time-dependent: 46 percent were successful prior to 1973, while only 25 percent were effective after that date. He reports that the Hufbauer and Schott data agree.

9. Homer E. Moyer and Linda Mabry, *Export Controls as Instruments of Foreign Policy: The History, Legal Issue, and Policy Lessons of Three Recent Cases* (Washington, D.C.: International Law Institute, University Press of America, 1985), 156-157.

10. A brief introduction to the history of international export control can be found in Czinkota, "International Economic Sanctions and Trade Controls: A Taxonomic Analysis," in *Export Controls: Building Reasonable Commercial Ties with Political Adversaries*.

11. Anthony T. Green, *U.S.-Japan Technology Transfer: Accommodating Different Interests* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-86-1, 1986), Table A, 7.

12. Ibid.

13. This supersedes Export Control Acts of 1969 (PL 91-184, 83 Stat. 841, December 30, 1969) and 1979 (PL 96-72, 93 Stat. 503, September 29, 1979).

14. Glennon J. Harrison and George Holliday, *Export Control*, Congressional Research Service, April 16, 1991, 7. H.R. 4653 was pocketed vetoed by President Bush because of disagreements on nonproliferation controls.

15. Ibid., 1.

16. 50 USC 2402(14).

17. 50 USC 2404(b)(1).

18. Ross L. Crown, "Supreme Court Avoids Constitutional Challenge to Export Control Act," *American Bar Association National Law Report*, **15**, 6 (June 1993), 3.

19. Hrach Gregorian, "Foreign Economic Sanctions As A Tool Of Foreign Policy: Short History of the U.S. Experience," *Private Property and National Security Foreign Economic Sanctions and the Constitution*, 5-7.

20. Interview with George Menas.

21. Defense Science Task Force, *An Analysis of Export Controls of U.S. Technology—A DOD Perspective*, report prepared for Department of Defense, Office of Undersecretary of Defense for Research and Engineering, Washington, D.C., February 4, 1976.

22. Green, *U.S.-Japan Technology Transfer*, Table 2-1, 7.

23. Interview with George Menas.

24. Harrison and Holliday, "Export Controls," 3-4.

25. Ibid.

26. Computerram International Access Company, "Soviet Focus; RISCs still banned, seem to be the one anomaly in the new liberal COCOM export rules," Aug. 14, 1991 [NEXIS].

27. In addition, the full list includes telecommunications; computers; navigation and avionics systems; propulsion systems; sensor systems and lasers; electronics design, development and production; advanced materials and material processing; and marine technology.

28. Harrison and Holliday, "Export Controls," 5.

29. Interview by the author with Walter Earle, Chief of COCOM Policy, Defense Technology Security Agency. Such countries as Iraq, North Korea, Vietnam, Libya, Syria, and Cuba fall under foreign policy controls and are not included in the COCOM restrictions aimed at the former Soviet Union and its allies.

30. Harrison and Holliday, "Export Controls," 7. The IEEPA can be applied only in a national emergency.

31. Ibid., 8.

32. "Soviet Focus; RISCs still banned" [NEXIS].

33. Specifically excluded from general licenses by the new regulations were supercomputers, cryptographic equipment, night-vision equipment, high-speed streak cameras, flash discharge, X-ray equipment, and items controlled for missile non-proliferation reasons.

34. Federal Information Systems Corporation Federal News Services, "Statement by the US Department of Commerce: Commerce Eases Licensing Regulations," April 23, 1992 [NEXIS].

35. International Trade Reporter, "U.S., Allies Agree to Ease Export Controls, Invite Ex-Soviet Bloc Nations to Join 'Forum,'" **9**, 23, June 3, 1992, 958 [NEXIS]. Margaret Tutwiler, then State Department Press Secretary, was quoted as saying that the aims of the forum will be to allow "significantly wider access" to those countries to advanced western goods and technology; to develop procedures for preventing the diversion of high-technology exports to military or other unauthorized end-users; and to improve cooperation on "matters if concern" on export controls.

36. Robert Kuttner, "How 'National Security' Hurts National Competitiveness," 141.

37. NAS, *Finding Common Ground*, 165, 250. The following is a complete list of the trends in technology that affect export controls identified in the study: (*i*) the changing structure of global economy; (*ii*) the increasingly rapid global diffusion of technology; (*iii*) declining U.S. technological and manufacturing preeminence; (*iv*) growing sophistication in technology and manufacturing sophistication in Japan and the newly industrializing countries; (*v*) the changing distribution of global economic and financial power; (*vi*) the weakening of the U.S. defense base; (*vii*) the growing importance of exports to the economic vitality of the U.S.; (*viii*) rapid technological progress, leading to the extension and "filling in" of the technological spectrum; (*ix*) globalization of the technologies, along with the increased international competition; (*x*) commoditization of many products, typified by low and steadily decreasing prices, high production volumes, a multiplicity of producers, and high degrees of substitutability of increasingly more powerful computer equipment.

38. U.S. Department of Commerce, *Statistical Abstract of the United States 1992* (Washington, D.C.: 1992), Table 1336, 804. Among the exports for that year were $26 billion in ADP equipment, $24 billion in airplanes, $17 billion in industrial machinery, $30 billion in electrical machinery, and $32 billion in various chemicals.

39. Kuttner, "How 'National Security' Hurts National Competitiveness," 141.

40. Interview by the author with Seymour Goodman, Chair, Computer Science and Technology Board, and member of the National Academy of Sciences Export Control Study (1991), Feb. 22, 1993.

41. Interview with S. Goodman.

42. Ibid.

43. DOD Directive 2040.2, *International Transfers of Technology, Goods, and Services and Munitions*, January 17, 1984, defines technology subject to export control as "The technical information and know-how that can be used to design, produce, manufacture, use, or reconstruct goods, including technical data and computer software. The term does not include the goods themselves."

44. Export Administration Regulations, 15 CFR 368, reprinted in Michael J. Ciffrino and Americo R. Cinquegranga, "Outline of Panel Discussion on Government Controls of Exports of Technical Information," in *Symposium on Transfer of Technology in the International Marketplace*, March 29-30, 1984 (Washington, D.C.: Federal Bar Association, 1984), 77-79.

45. Nick Wrenden, "Prior Restraint and the Progressive," *Freedom of Information Center Report No. 466*, School of Journalism, University of Missouri at Columbia, October 1981, P.1-P.2.

46. Stuart Macdonald, *Technology and the Tyranny of Export Controls Whisper Who Dares*, (London: Macmillin, 1990), 71; Table 5.1 lists some scientific conferences that foreign scientists were barred by the EAR.

47. USC §2404(6)(b)(1).

48. NAS, *Balancing the National Interest*, 160-161.

49. USC §2403(c) states that "the President shall not impose export controls for foreign policy or national security purposes on the export from the Unites States of goods or technology which he determines are available without restriction from sources outside the United States in sufficient quantities and comparable in quality to those produced in the United States so as to render the controls ineffective in achieving their purpose, unless the President determines. . .that the absence of such controls would prove detrimental."

50. *Finding Common Ground*, 175.

51. Exceptions include supercomputers, cryptographic equipment, night-vision equipment, high-speed streak cameras, flash-discharge X-ray equipment, items controlled for missile nonproliferation reasons, in addition to items on the munitions and atomic energy lists.

52. 50 USC §2404(k) outlines the rules for bilateral agreements between the U.S. and other countries on export control: if "agreements on export restrictions comparable in practice to those maintained by the Coordinating Committee, the Secretary shall treat exports, whether by individual or multiple licenses, to countries party to such agreements in the same manner as exports to members of the Coordinating Committee are treated."

53. *Balancing the National Interest*, 157.

54. *Finding Common Ground*, 172.

55. Interview with George Menas.

56. Interview by the author with Fred Demech, TRW, Dec. 11, 1992; *Finding Common Ground*, 160, 175.

57. *Finding Common Ground*, 158.

58. Interview with S. Goodman.

59. EAR 15 CFR Part 768, 1-1-92 Version. One example from the first page of the CCL shows the complexity of the regulations:

1A02A "Composite" structures or laminates
Validated License Required: Non-COCOM countries
List of Items Controlled
a. Having an organic "matrix" and made from materials embargoed by 1C10.c,d. or e; or
b. Having a metal or carbon "matrix" and made from:
b.1. Carbon "fibrous and filamentary materials" with:
b.1.a. A "specific modulus" exceeding 10150000m; or
b.1.b. A "specific tensile strength" exceeding 177000m; or
b.2. Materials controlled by 1C10.c
Related ECCNs: See 1A22B for missile controls on "composite" structures or laminates, not controlled by 1A02A, that are usable in "missile" systems.

60. *Balancing the National Interest*, 163-164.

61. Ibid., 92. As part of the Omnibus Trade and Competitiveness Act, the Multilateral Export Control Enhancement Amendments Act (MECEAA), 102 Stat. 1364-70, §2441-47, was passed in response to the Toshiba-Kongsberg Incident, amending the EAA to strengthen the sanctions against companies violating export controls. The MECEAA allowed the president to apply sanctions of two to five years against either individuals or companies that violate COCOM rules that result in substantial enhancement of Soviet and eastern bloc capabilities. The sanctions shall apply to any foreign persons, as well as any parent, affiliate, or subsidiary. The sanctions prohibit contracting with and procurement of products from sanctioned persons by the government and an prohibition on importation into the U.S. of all products produced by the sanctioned person. The president has the authority to limit the sanctions where necessary to national defense, if the affiliates did not knowingly violate COCOM rules, or no substantial enhancement occurred.

62. Seymour Goodman, Chairmen of Computer Science and Technology Board and member of the 1991 National Academy of Sciences Export Control Study, interview with the author, February 1993 stated that the penalties "are only effective against the little guy who attempts to play by the rules. It is ineffective against anyone who is out to break the rules."

63. Stephen D. Kelly, *Curbing Illegal Transfers of Foreign-Developed Critical High Technology from COCOM Nations to the Soviet Union: An Analysis of the Toshiba Kongsberg Incident*, Boston College International & Comparative Law Review, Vol XII, No 1, Winter 1989.

64. Ibid., 185.

65. Ibid., 183. Total damages are expected to be in the billions.

66. Ibid., 184.

67. Ibid., 206-207.

68. National Academy of Sciences, *Balancing the National Interest*, 164, and *Finding Common Ground*, 173; also interview with Fred Demech.

69. Interview by the author with Ronnie L. Goldberg, Senior Vice President Policy and Program, USCIB, Feb. 7, 1993. According to Goldberg, industry generally accepts in principle the need for continued export control, although her impression of industry thoughts based on issues brought to USCIB was that the lists were still too long and policies have not kept pace with the dramatic geopolitical changes that have affected U.S. national security. Increased consultation with industry would help to eliminate the problem of the lists.

70. 50 USC §2404(f)(1)(A).

71. *Balancing the National Interest*, 156.

72. Ibid., Appendix D, 266; also, Office of the Undersecretary of Defense for Policy, *Assessing the Effect of Technology Transfer on U.S./Western Security—A Defense Perspective* (Washington, D.C., February 1985).

73. National Academy of Sciences, *Balancing the National Interest*, Table 5-1, 121.

74. Interview with R.L. Goldberg; also, Kuttner, "How 'National Security' Hurts National Competitiveness," 141, and Martin J. Hillenbrand, "Export Control Policy in the 1990s: The Diplomatic Perspective," in *Export Controls in Transition: Perspective, Problems, and Prospects*, edited by Gary K. Bertch and Steven Elliot-Gower (Durham: Duke University Press, 1992), 63.

75. Interview with G. Menas; interview with S. Goodman, who stated that the NAS authors told him during his committee studies "that they wished that the figure had not been published because they had no independent support of the numbers used in the study." The NAS report itself concluded (p. 165) that "a comprehensive empirical analysis of the costs and benefits of controls currently is precluded by the lack of data, by the complexity of the system, and by a variety of qualitative judgements that must enter into an evaluation."

76. *Assessing the Effect of Technology Transfer on U.S./Western Security—A Defense Perspective*, Fig. 3-10, p. 3-22, and Fig. 3-11, p. 3-23.

77. Macdonald, *Technology and the Tyranny of Export Controls*, 92.

78. Ibid., 93.

79. Interview with S. Goodman.

80. Macdonald, *Technology and the Tyranny of Export Controls*, 93.

Chapter Six

Technology Limitations

6.1 Commercial Development of Technology

The secrecy of national security technology can be lost through commercialization. Export control cover technology explicitly transferred to other countries, but because technology can be transferred in many other ways, the government also needs other mechanisms of technology control. Dual-use technology developed for military purposes provides especially tough issues. This chapter discusses the policy issues of two national security technologies, commercial cryptography[1] and photographic satellites. Other technologies, such as atomic energy, have also been restricted, but these examples highlight many important questions raised by attempts by the national security establishment to protect these particular technologies.

The national security community controlled access to them, because they were essential parts of its system. Secrecy was not controversial, because the technologies remained classified and because there were no commercial or societal objectives to balance. Eventually, society, which had many of the same needs as the military, discovered the usefulness of these dual-use technologies and pressured industry to produce them commercially. Industry either rediscovered the military technologies or converted the classified technologies to a commercial setting. Unlike other critical technologies, for example, computers and telecommunications, which had always been dual-use and were restricted through export control, these military technologies had not been commercially exploited owing to government resistance. Unable to prevent commercialization, the government tried to limit or delay widespread introduction of these technologies into the marketplace, claiming that the risk to national security outweighed the benefits commercialization might provide.

The government affected the spread of these technologies in several ways: classification, secrecy patents, export control, and statutory limits. It also used nonregulatory approaches, such as voluntary prepublication review, that gave authority to fund research grants to the DOD and allowed participation by the DOD in defining standards for disputed commercial

technology, which prompted proponents of a technology to fear future restrictions. Such examples demonstrate possible restrictive practices.

The examples in **Chapter Two** were developed by the government for national security purposes, without commercial exploitation.[2] Among the reasons for their limited commercial appeal were a small commercial market, inability to meet basic consumer requirements, unattractive costs per unit, or costs of initial development costs too high to receive an adequate investment return. Because the military did not demand cost efficiency and because the technologies supplied critical national security benefits, the government invested in the basic technologies and in their underlying infrastructure. After the military had successfully developed and exploited the technologies for a number of years,[3] society "discovered" them. A commercial market began to develop, because the benefits—private communications or increased knowledge of the world—were important also to the public and the advancing sophistication of technology overcame many cost inefficiencies.

Commercial development proceeded by redeveloping government technologies, taking advantage of previous research and better methods to reduce the cost of production and converting declassified military technologies to civilian use. Technology redevelopment, such as commercial cryptography, is completely unclassified and did not require active government participation to promote commercialization. The redevelopment of cryptography proceeded rapidly in both academic laboratories and commercial industry once computers enabled cheap, fast, secure algorithms and society needed protection for commercial and individual communications. On the other hand, defense conversion requires active government participation to provide national security technologies to private industry for commercial products. In the example of the photographic satellites, the necessary launch, space, photographic, and communication technologies all were developed in a classified environment. Various components have been declassified over the years, transferred to industry for other purposes, such as telecommunications satellites, and then reengineered into commercial photographic satellite technology.

6.2 Basic Issues

The basic issue is the goal or aim of placing limits on technology. One problem is that once a technology is known to exist and anyone has a reason to recreate it, it can be restricted

and its spread delayed for a short while. The debate must center on the benefits of delaying the growth of technology as opposed to the corresponding costs of such delay.

6.2.1 National Security

Although extensive commercial exploitation of formerly military technologies is possible, many important national security considerations continue to complicate this issue. The tradeoffs inherent in the decisions made about the level of technology and its rate of development must be understood. The government thinks that unregulated commercial exploitation of these technologies will damage national security. Although some foreign governments have national security technologies equivalent to those of the U.S. and thus do not stand to benefit from technology transfer, U.S. commercial products in these technologies are better than those many other governments possess. Exploitation, the U.S. government argues, even if limited, would improve the technologies available to many foreign adversaries and hurt U.S. national security. Because the U.S. does not have a monopoly on these technologies, opening a market would also set up a commercial battle with the other advanced countries to develop and market the best products, improving the available technology even more quickly. These problems are not restricted to commercial products, which can be protected through export control; technology transfer can occur without the development of commercial products. Published research, as in articles that describe new cryptographic algorithms, techniques, or publication of a commercial patent, can provide information useful to foreign countries.

These examples indicate how exploitation of formerly military technologies can damage the national security interests of the U.S. Commercial cryptography, developed by either a U.S. company or a foreign one, can protect information belonging to other countries, including those hostile to the U.S., from U.S. intelligence. Academic discussion of cryptography could lead to better understanding of cryptography and development of indigenous algorithms or techniques to attack U.S. communications, government and commercial. Photographic satellites could be used to perform intelligence gathering on the U.S., for military and commercial purposes. Adversarial governments will save far more by purchasing U.S. commercial products instead of independently developing their own than U.S. companies will gain from sales of the products to them.

The question of national security is not so simple. Although some aspects of national security might be damaged by increasing commercial use of these technologies, in other areas their use might benefit U.S. national interests. Widespread use of commercial photographic satellites might lessen regional tensions, because if countries could monitor their neighbors better, the chances of surprise attacks might be lessened.[4] Economic competitiveness might improve through better protection of U.S. commercial communications.

6.2.2 Economic Considerations

The primary argument against technology restrictions is economic. If the U.S. does not exploit a particular technology, given no shortage of technologically sophisticated countries, other countries could exploit it,[5] causing the same harm to U.S. national security discussed above (**section 6.2.1**).[6] Once a market niche is identified, products will be developed to fill it, regardless of the government's wishes. Both cryptography and photographic satellites have already developed niches; should U.S. industry, which in 1993 leads in these technologies, forgo an economic opportunity? If the government were to try to prevent U.S. exploitation of them, foreign competition would certainly fill the market, making it unlikely that in the future U.S. companies would be competitive, even if, later on, the attitude of the government were to change. If such technologies as cryptographic enforced privacy are considered necessary for economic competitiveness, should U.S. industries be forced either to use an inferior technology or to buy superior products from a foreign source?

What right does government have to interfere with commercial development? It supports the technology development it believes is in the public interest, through R&D grants, government contracts, tax subsidies, and technology transfer programs. Although it can express disapproval of selected technology developments by not granting these benefits, does it have the right to go further and actively try to suppress the technologies? Why should government hold greater privilege to interfere in technology development than it does to intrude into other nongovernmental legal functions that it may disapprove of? Regardless, the government uses (or at least appears to use) its broad national security discretion to delay advancement of certain technologies beyond minimal technical levels.

6.2.3 General Issues

Absolute national security does not exist, because the U.S. could not bear the cost, either economically or politically. Prudent risk management is necessary in every decision about national security. The best solution is to find a compromise that the technology meets commercial requirements while it does not introduce an unacceptably large national security risk. Unfortunately, even if such a compromise were to exist, achieving widespread agreement might not be possible, because the different sides argue from different perspectives. The government believes that national security can be balanced with the needs of society and that "adequate" technology is sufficient for the public, while advocates of commercialization argue that anything less than state-of-the-art technology harms society.

As this chapter was written, the technologies examined here were in dispute. The dual-use implications of large sectors of the economy can be exploited by other countries with serious repercussions for U.S. national security, yet the commercial presence of most national security technology is so large that the economic impact of limiting the technology would be extremely negative. Because dual-use technologies—telecommunications, computers, aeronautics, and electronics—were recognized as having important commercial benefits, they were developed by both the military and commercial sectors.[7] A central concern is why society benefits from one technology but not from others. Are there considerations beyond historical accident that make limiting technologies like cryptography more critical than limiting dual-use technologies like computers, or considerations that make commercially exploiting some dual-use technologies particularly important, even though such exploitation may damage the national security?

To date, public arguments on the tradeoffs have proved unsatisfactory. The government contends that classification concerns prevent it from properly articulating details on national security damage that might result from full commercial exploitation and from refuting public criticism. Such reticence tilts the argument toward commercial interests, which can make a case for economic damage from restrictions. The government comes out looking very heavy handed, because all it can say is, "Sorry, for the good of country, industry must sacrifice," without providing a convincing justification.[8]

6.3 Commercial Cryptography

Commercial cryptography provides the first example of a technology the government is accused of trying to control unnecessarily. According to the dictionary definition, cryptography is the process or art of writing in secret characters or in cipher, and it has been used for thousands of years to protect critical military and commercial information. Although a commercial market for cryptography has always existed,[9] a small one because equipment was expensive and slow. Until World War II, commercial cryptography was reasonably close to the level of military cryptography.[10] Because of the benefits gained by the U.S. in breaking the German and Japanese codes, signals intelligence and communications security became critical military technologies. After the War, the government allocated large resources to cryptography, and its technological ability moved far ahead of industry. Commercial cryptography remained a small market, however, because equipment remained expensive and slow, the amount of traffic in need of protection small, and the fear that data might be intercepted low.

6.3.1 Cryptography Requirements

Improvements in computer technology and the advent of large communication networks increased the commercial need for encryption equipment. Computers allowed fast encryption, networks passed substantial amounts of sensitive data that needed protection, and network design allowed data to be intercepted easily. According to the findings of a recent (1987) OTA study that highlighted the general need for cryptography:

> Today's public communication network is, for the most part, at least as easy to exploit as at any time in the history of telecommunications. The design of the public switched network is such that some parts of it are vulnerable to relatively easy exploitation (wiretaps on copper cable, over-the-air interception), while others (e.g. fiber optic cable) present greater inherent barriers to exploitation.
>
> There are, and will likely remain, opportunities for casual, generally untargeted eavesdropping of communications. However, targeted and consistently successful unauthorized access requires greater resources. For systems with sophisticated safeguards, the resource requirements may frustrate even the efforts of national intelligence agencies. However, adversaries with sufficient resources can eventually defeat all barriers except, perhaps, those based on high-quality encryption.[11]

The study went on:

> Encryption is the most important technique for improving communications security. . . . Good-quality encryption is the only relatively sure way to prevent many kinds of deliberate misuse in increasingly complex communications and computer systems with many access points.[12]

It concluded that "To achieve most of the above, cryptography is critically important. There are no close substitutes for cryptography available today."[13]

The study identified the following as possible applications for cryptography:

- protecting information communicated over a transmission medium,
- protecting information during storage on a computer or other storage media,
- ensuring the integrity of information during transmission or storage,
- ensuring the authenticity of the transmitting and receiving ends of a communication, and
- computer security applications, such as access control.

Each of the application is equally necessary to national security and commercial applications.

6.3.2 The Role of NSA

Defining a rational policy for commercial cryptography, for example, has proved difficult. The government agency with primary responsibility for cryptography policy, the NSA,[14] has a difficult balancing job. Its responsibilities for conducting signals intelligence, protecting U.S. national security communications, and, under the Computer Security Act of 1987, for working with the National Institute of Standards and Technology (NIST) on techniques for protecting unclassified civil computers and communications often conflict. Its almost complete control over classified government cryptography and its almost complete exemption for NSA information that is sensitive or classified and thus witholdable under the FOIA,[15] effectively allow the NSA to control the release of information about its own operation. NSA is also the only agency allowed to declassify information concerned with cryptographic material,[16] which prevents interagency battles over releasing cryptographic technology. Critics feel that its heavy involvement in commercial cryptography, while, as part of the intelligence community, the NSA has special channels of accountability, is inappropriate.[17]

The NSA is perceived by the academic and commercial communities as too concerned with its intelligence mission and hostile to open research on cryptography. The NSA's thinking about public research in cryptography was expressed by Admiral Bobby R. Inman in

1979 in a speech to the Air Force Communications and Electronics Organization (AFCEA) that raised the same national security concerns still debated in 1993:

> The agency's sole consideration is the detrimental effect on the Agency's mission, and thus on the security of the United States, that would result from the proliferation abroad of sophisticated cryptologic technology. . . . Application of the genius of the American scholarly community to cryptographic and cryptanalytic problems and widespread dissemination of resulting discoveries, carries the clear risk that some of NSA's cryptanalytic successes will be duplicated, with a consequent improvement of cryptography by foreign targets. No less significant is the risk that the cryptographic principles embodied in communications security devices developed by the NSA will be rendered ineffective by paralleled non-governmental cryptologic activity and publication.[18]

Classification has been used to keep government secrets protected, but reclassification has also been used to try to prevent diffusion of public information. Recent cases of reclassification of public data, based on the authority of E.O. 12356, involved James Bamford and John Gilmore. In the early 1980s, after publication of *The Puzzle Palace*, a book critical of the NSA, the government reclassified some of the research material at the George Marshall Library that had been used in the book.[19] More recently, the NSA tried to retrieve and reclassify material written by William Friedman from an independent researcher, John Gilmore, asserting that it was still classified, but Gilmore claimed he had found it in a public library with a declassification stamp dated 1977.[20] The NSA reversed itself in 1992 and settled the matter by officially declassifying the material.[21]

The NSA also tried to used the Invention Secrecy Act to control private research into cryptography. In 1978, because of requests by the NSA, the patent office placed secrecy orders on two inventions, both developed without government sponsorship or information. The first invention was by George Davida for a nonlinear stream cipher device developed on a grant from the National Science Foundation (NSF). After public protest by Davida and by Werner Baum, chancellor of the University of Wisconsin, the order was lifted. The second invention involved the development of a "phaserphone" by four Seattle businessmen. Again, after public protest, this secrecy order too was revoked.[22] Since then, no secrecy patents have been requested for nongovernment cryptographic products. Although the NSA changed its patent review process after these incidents, the practice of sending relevant patent requests to the NSA for review continues.[23]

The NSA interacts with the academic research community in ways that raise fears that the agency will subtly stifle research. First, it participates in the grant reviews of the NSF, which funds much academic scientific research and started to supply cryptographic grant funds and in 1978 started supplying for NSA review all grant requests for cryptographic research. In 1981 NSA was granted authority to supplement NSF grants by partially funding the grant or providing independent grants.[24] Questions of scientific independence naturally arise, because the funding agency has a least the appearance of a conflict of interest in the outcome of the research.

The NSA and the scientific community have agreed on a voluntary prepublication review procedure for cryptographic research.[25] Following public furor over the NSA's perceived attempt to suppress public research through secrecy orders, Adm. Inman attempted to find a compromise between the government's position and that of researchers. His AFCEA speech, the first public speech by a director of the NSA, outlined the agency's concerns about public research and asked the academic community for cooperation.[26] In response, the American Council on Education set up the Public Cryptographic Study Group, chaired by Werner Baum, to study the issues raised by public research. The group consisted of government representatives and researchers, such as George Davida,[27] who had been involved in the patent controversy. In its 1981 report, the group recommended, over Davida's objections,[28] the establishment of a voluntary requirement for researchers to submit papers to the NSA for prepublication review. The NSA could then recommend changes in a paper, but researchers were not obligated to follow the recommendation.[29] The system, although not perfect,[30] remains in effect in 1993, and there are few implementation problems. Most researchers submit their papers, the NSA only requests modifications in rare instances, and, in almost all cases, researchers have followed the NSA's recommendations.[31] Public research in cryptography has not been unduly inhibited by prepublication review.

6.3.3 Cryptographic Standards

The best known and most far-reaching efforts by the NSA to control the level of public technology involve defining cryptography standards. In 1973 the National Bureau of Standards (NBS), since renamed the National Institute of Science and Technology (NIST), began to develop a public cryptography standard for nongovernment and unclassified information. After soliciting proposals, NBS, with NSA input, chose an IBM design. The NSA requested

two changes in the design, a modification of the underlying cryptography algorithm and a abbreviation of the key length. Critics objected to the resultant Digital Encryption Standard (DES), because they felt that the changes weakened the algorithm. They felt, too, that the shorter key enabled NSA to read the information through brute force and that the agency might have put a trap door into the algorithm to ease cryptanalysis.[32] So far these fears have proved unfounded, DES is widely used in the 1990s, and no cryptographic flaws have been found. When in 1987 the NSA tried to decertify DES as a federal standard, the "outcry and intense pressure from government, the financial industry and other commercial cryptography users"[33] forced it to back down and recertify DES.

In 1991, NIST published the Digital Signature Standard (DSS),[34] a public cryptographic standard for electronic signatures, and the NSA was heavily involved in its development.[35] Many of the same issues raised about DES in 1977 concerning the algorithm resurfaced with regard to DSS. Critics complained that the key length was too short, weakening the algorithm, that the NSA's involvement was a conflict of interest and caused the weakening of the algorithm, that the NSA might have placed a trap door in the algorithm to ensure that it could exploit the cryptography, and that the secret nature of the development of DSS prevented independent verification.[36] A complaint unique to DSS was that the NSA was trying to prevent widespread utilization of RSA,**** a public, commercially licensed algorithm that can implement electronic signatures. Proponents of RSA believe that, prior to release of DSS, it was on its way to becoming a de facto standard. Critics claim that the NSA introduced DSS specifically to supplant RSA, because the RSA algorithm prevented the NSA from reading traffic encrypted under RSA.[37] A potential conflict of interest must be noted: many of the most vocal critics of the DSS proposal, including Dr. Ronald Rivest, one of the inventors of RSA, have a financial interest in RSA that might be affected by widespread use of DSS.[38]

The NSA also participated in the development of a third standard. On April 16, 1993, President Clinton announced the introduction of the controversial "Clipper Chip,"[39] developed by NIST with extensive NSA support.[40] The chip was designed to protect telephone communications while preserving the government's ability to tap communications.

****The Rivest-Shamir-Adelman algorithm.

The president said that the Clipper chip was an attempt to balance "the privacy of our citizens. . . the ability of authorized officials to access telephone calls and data. . .[and] the need of U.S. companies to manufacture and export high technology products."[41] At the time of this writing, the controversy has centered on use of the chip in government wiretapping, not its cryptographic implications. **Chapter Eight** discusses the civil liberty issues raised by the chip.

6.3.4 Export Control Restrictions

Export control is a major impediment for commercial cryptography products. Cryptography can be divided into two categories: (*i*) those that protect information, such as DES, and (*ii*) those that authenticate it, like DSS. Protective cryptography is categorized as a munition by the ITAR and subject to export control, while the controls on authentication cryptography either are nonexistent or significantly reduced.[42] Because the NSA has the expertise of the DOD in cryptography, it participates in the export control decision along with the departments of State and Commerce. Export of cryptography is not totally banned, but all proposed sales are reviewed on a case-by-case basis. Although knowledge of the underlying algorithm allows production, public knowledge of it does not exclude the product from export controls. Export controls are in place on the largest selling commercial cryptographic products, which use the RSA and DES algorithms.[43] Products that implement authentication and integrity functions can be exported, but not privacy applications.[44] Some DES licenses are granted also for sales to international financial organizations and to overseas affiliates of U.S. firms.[45] As of June 1993, the export control status of DSS and the Clipper chip have not been determined.[46] Export control limits the commercial cryptography market for U.S. companies, which can sell only to other U.S. companies. Export control restrictions often require U.S. companies to develop two versions of a product, one with encryption for internal U.S. consumption and another without it (or at least with a different algorithm) for export.[47]

6.3.5 Costs

The tradeoffs between the economic cost to industry and public damage from cryptographic restrictions versus the loss of national security information have received little scholarly attention. A Carnegie-Mellon study concluded in 1980 that the "net social benefit" from public encryption changed on the basis of the size of the commercial market for encryption. It said that in a large market, with most commercial interests using encryption to

protect their data, the benefit to the economy offset national security losses. If, however, the majority of business community did not use encryption, the loss of national security offset the economic benefits.[48] In 1993, the commercial encryption market is still relatively small,[49] and whether the conditions brought about by the end of the Cold War will change the study's fundamental conclusions needs further work.

6.4 Photographic Satellites

Photographic satellites offer the second example of a national security technology the government is accused of controlling. Commercial satellites raise a different set of questions from those raised by cryptography, because the government has the power to regulate satellite technology. The Landsat Act requires the government to license any commercial remote-sensing satellite before launch, and foreign sales are controlled through export control laws. The U.S. policy toward photographic satellites was defined in the classified Presidential Directive 37, issued by President Carter in 1978, which specified ten meters as the maximum resolution level for commercial satellites.[50]

Commercial photographic satellites are a small but growing international market. The use of space photography, for such activities as land utilization and news, is increasingly prevalent. For example, in 1986 the media employed imaging from the French satellite SPOT during the accident at the Chernobyl nuclear reactor.[51] Currently, three satellites provide commercial imaging, the U.S. Landsat V with thirty-meter resolution, the French SPOT, with ten-meter resolution,[52] and a Russian satellite with two-meter resolution.[53] The next generation Landsat, scheduled for launch in 1995, will have two-meter resolution.[54] None of these satellite systems is entirely commercial. The U.S. government has an interest in Landsat, although ownership was transferred to a commercial company, EOSAT, in 1985.[55] The SPOT and the Russian systems are at least partly owned by their respective governments.[56] In all three instances, the government that owns the satellite reserves the right to refuse to sell any photograph that hurts its national security.

A second market for photographic satellites is international security. Only a few high-technology countries, such as the U.S., France, Japan, Russia, and China,[57] possess the ability to build high-resolution satellites, but many other countries want this type of intelligence. Three countries, the United Arab Emirates,[58] South Korea, and Spain,[59] have

offered to buy one-meter photographic satellites from the U.S., which, if sold, would not be replicas of existing intelligence satellites but would incorporate commercial versions of military instruments. Commercial photographic satellites are potentially a multibillion dollar industry, with an estimated price tag of several hundred million dollars for a one-meter satellite.[60] The U.S. will not retain a monopoly over very-high-resolution satellites for long. The French developers of SPOT are developing a new spy satellite, the Helios, with one-meter resolution, scheduled for launch in 1994.[61]

6.4.1 Benefits

Advocates for unrestricted use of commercial satellite technology point to its economic benefits, both in the sale and the potential for gaining economic intelligence. There are enough countries and organizations wanting high quality space photography that a commercial market can probably succeed. As of 1993, the U.S. does not control the market for photography because of the better quality of foreign competition. The availability of foreign satellites will satisfy the demand for high-resolution imaging, regardless of the U.S.'s national security interests. Potential customers for space photography include the news media and commercial firms trying to keep track of their competitors. U.S. relaxation of satellite restrictions would enable U.S. firms to compete for the hundreds of millions of dollars the satellites would cost to develop, deploy and operate. Satellite sales would help the aerospace industry, a critical national security industrial sector, stay stable and competitive in spite of reduced military spending. For example, Litton Itek Optical, a potential producer of commercial satellites, recently laid off one fourth of their staff due to reduced defense contracts.[62]

There are potential national security benefits from American participation in commercial satellites. U.S. ownership of the satellites serves two objectives, allowing the U.S. to control access to imagery that might damage the U.S. national security as well as ensuring that foreign governments could not deny access to U.S. interests.[63] If only foreign satellites existed, the satellites could take and distribute pictures that harm the U.S., like detailed pictures of military installations. Likewise, foreign owners of satellites could deny access to imagery that would be useful to U.S. companies against their own companies.

Satellites could also reduce international tensions. Imagery could help prevent war by eliminating the fear of successful surprise attacks by neighboring countries. It could give diplomacy a chance to defuse threatening situations without war. Others suggest that this won't happen because "it can just as easily scout invasion routes and targets." [64]

6.4.2 National Security Effects

The national security community is naturally worried about the effect on the U.S. economy and national security of high-resolution satellites. Although the proposed commercial resolutions are far short of the military satellites, which in the late 1970s had an estimated resolution of .15 meters,[65] they are good enough to provide an adversary useful intelligence about the U.S. Five-meter resolution (16.5 feet) can detect troops and aircraft, identify surface ships or surfaced submarines, and precisely identify specific terrain, such as roads and harbors. One-meter resolution allows detection of artillery, rockets, and vehicles, identification of nuclear weapon components, and precise identification of troops, aircraft, command and control locations, and surfaced submarines.[66]

There are other national security concerns related to permitting the development of commercial satellites or selling intelligence satellites:

- transfer of satellite technology to the buyers of commercial satellites permitting the buyer to build their own satellites;
- the intelligence could be shared with countries hostile to the U.S. or be used to produce military or economic intelligence against the U.S.; and
- the intelligence could upset diplomacy by forcing the government to acknowledge national security events instead of using "secret negotiations."

To protect itself, the U.S. would structure any sale to eliminate these problems. In a requested sale to the United Arab Emirates in 1993, the U.S. proposed that the satellite "would be launched from a US booster from US territory and the US contractor would operate the spacecraft." Further, the "governments would negotiate a set of agreements restricting the emirates' use of the satellite for intelligence purposes and prohibiting them from selling data on a commercial basis."[67] An additional concern about personal privacy enters with better resolution: at a high enough resolution, maybe one-meter, some personal effects of individual people may be identified. If the resolution necessary to read the

proverbial license plate is ever reached, significant privacy issues would need to be addressed.[68]

With passage of the Land Remote-Sensing Commercialization Act of 1984, the government had the power to enforce resolution limitations administratively. Likewise, until recently it controlled the launch facilities and could refuse to launch any satellite it believed damaged national security. Now, foreign launchers—including the Europeans, Russians, and Chinese[69]—can take U.S. satellites into orbit, regardless of concerns about U.S. national security. Because of uncontrollable foreign competition, unilateral U.S. limitations on development and deployment of higher resolution commercial satellites is no longer achievable. Government agencies, reflecting their conflicting missions, are divided on the issue of how far to permit satellite technology to develop. Within the Bush administration, the Treasury and Energy departments pressed for liberalized rules, while State, Defense, and Interior as well as the NASA urged against it.[70] Landsat VI will be the first U.S. commercial satellite under the ten-meter limit, thus reflecting the changing world situation.

Notes

1. A slightly dated yet detailed look at the questions raised by commercial cryptography is found in Tom Ferguson, *Private Locks, Public Keys and State Secrets: New Problems in Guarding Information with Cryptography* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, 1982, P-82-5).

2. In the case of commercial cryptography, this is an overgeneralization. Versions of commercial cryptography had always been around to protect business communications. Since World War Two, the government, devoting considerable resources to cryptography, had developed it far beyond its commercial equivalent. The problems discussed in this chapter began when commercial cryptography started to bridge the gap that had been created and began to get closer to the level of the government.

3. The cost of developing these technologies is classified. The operating budget for the NRO, which operates the satellites, was approximately $5 billion in 1992, and the NRO has been in existence since 1960. Steven Aftergood, "NRO Declassified," *Secrecy & Government Bulletin*, **15** (October 1992), 1.

4. Interview by the author with Larry Cox, Staff Member, House Intelligence Committee, April 12, 1993.

5. The Computer Business Equipment Manufacturers Association (CBEMA) has documented the availability of DES encryption equipment in Russia as well as in other countries; interview by the author with Anne Urban, CBEMA, April 11, 1993. A product called Crypto II, which contains both the RSA and DES algorithms, can be bought for $5.00 in St. Petersburg; see John Perry Barlow, "Decrypting the Puzzle Palace," *Communications of the ACM*, **35**, 7 (July 1992), 7.

6. Allies of the U.S. are having the same problems with regulating cryptography. The Europeans are trying to prevent inclusion of state-of-the-art cryptography in European Community (EC) networks in order to allow government tapping. According to John Blau, in "Less-Secure GSM on Tap" (*CommunicationsWeek*, [April 19, 1993], "Europe's mobile telephone industry is developing less-secure GSM digital cellular equipment to mollify government law-enforcement agencies and adjust to restrictions on high-technology exports."

7. Alic et al., *Beyond Spinoff*, 64-75.

8. Interview by the author with Clinton Brooks, NSA, Jan. 29, 1993.

9. U.S. Congress, Office of Technical Assessment (OTA), *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*, OTA-CIT-310 (Washington, D.C.: U.S. Government Printing Office, October 1987), box A, p. 25. In 1845, a year after the invention of the telegraph, the first commercial algorithm for protecting telegraph messages was published. A commercial voice scrambler was patented within five years of the first demonstration of the telephone.

10. David Kahn, *Kahn on Codes: Secrets of the New Cryptography* (N.Y.: Macmillin, 1983), 78. The German Enigma machine, the main German cryptographic device used in the World War II, was a modification of a commercial device invented by Dr. Arthur Scherbius.

11. *Defending Secrets, Sharing Data*, 23.

12. Ibid., 54.

13. Ibid., 53.

14. NSA was first established in 1952 in a classified Presidential Directive. Its unclassified responsibilities were spelled out more clearly later, in E.O. 11905, Feb. 18, 1976.

15. James Bamford, in *1984: Civil Liberties*, 37. According to an NSA employment authorization bill (PL 86-36), "Nothing in this act or any other law shall be constructed to require the disclosure of the organization or any function of the National Security Agency, or any information with respect to the activities."

16. Interview with M. Levin.

17. "Documents Suggest NSA Dominated Encryption Plan," *Telecommunications Reports* (May 10, 1993), 32. According to this article, the CPSR (Computer Professionals for Social Responsibility), a civil liberties advocacy group that denounced the NSA's involvement with commercial cryptography, was quoted as saying that "Congress intended to remove NSA from the process of developing civilian computer security standards and to place that responsibility with NIST, a civilian agency. Congress expressed a particular concern the NSA, a military-intelligence agency, would improperly limit public access to information in a manner incompatible with civilian standard-setting."

18. Admiral Bobby R.Inman, speech to AFCEA, Jan. 11, 1979; quoted in Ferguson, *Private Locks, Public Keys*, 33-34.

19. Bamford, *1984: Civil Liberties*, 38.

20. John Markoff, "NSA Shrugs at Found 'Spy' Data," *New York Times*, Nov. 28, 1992, 8.

21. [Associated Press], "US will declassify 2 code texts," *Boston Globe*, Nov. 27, 1992, 16.

22. Kahn, *Kahn on Codes*, 199.

23. Ferguson, *Private Locks, Public Keys*, 25-27. "[National Security] Agency officials stress that they expect only a very tiny fraction of all patent applications will ever be considered for such orders; members of the review board [set up as part of the new procedure] must act affirmatively to maintain existing orders or issue new ones—the burden is on the reviewers to prove why the secrecy orders should not be rescinded."

24. Ibid., 29-32.

25. Schwartz, "Scientific Freedom and National Security: A Case Study of Cryptography," in *Striking a Balance*, 68.

26. Ferguson, *Private Locks, Public Keys*, 33-34.

27. Schwartz, "Scientific Freedom and National Security," 70.

28. Davida, in *1984: Civil Liberties*, 94.

29. Ferguson, *Private Locks, Public Keys*, 53-56.

30. One example of a researcher failing to follow NSA's requests involved John Gilmore, who, in June 1989, distributed copies of a paper written for the Xerox Corporation after NSA asked the company not to publish the document. Markoff, "NSA Shrugs at Found 'Spy' Data," 8.

31. Interview with Mike Levin.

32. Kahn, *Kahn on Codes*, 196.

33. "Public-key, GOSIP and Other NIST News," *Info Security News*, Jan.-Feb. 1993, **4**, no. 1.

34. Digital Signature Standard, 56 Federal Register 169, Aug. 30, 1991.

35. John Adams, "Cryptography=Privacy," *IEEE Spectrum*, **29**, 8 (August 1992), 29.

36. "Responses to NIST's Proposal," *Communications of the ACM*, **35**, 7 (July 1992), 41-49.

37. Ibid.

38. Two articles criticizing the DSS proposal were published in *Communications of the ACM* by two senior public researchers, Dr. Ronald Rivest and Dr. Martin Hellman. Dr. Rivest, a coinventor of the RSA algorithm, works for RSA Data Security, which markets RSA; Dr. Hellman was hired by RSA Data Security after he wrote his comments. Roger Schlafly, "Letters to the Editor," *Communications of the ACM*, **35**, 11 (November 1992), 20.

39. White House, "Statement by the Press Secretary," April 16, 1993, 1.

40. "Documents Suggest NSA Dominated Encryption Plan," *Telecommunications Reports* (May 10, 1993), 33.

41. White House Statement, April 16, 1993, 2.

42. Adams, "Cryptography = Privacy."

43. Ibid., 32-35.

44. System Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, "Computers at Risk: Safe Computing in the Information Age," in *Proceedings from the 1991 Cryptography and Privacy Conference, June 10, 1991* (Washington D.C.: National Academy Press, 1991), 155.

45. Telephone conversation of the author with an official of the NSA, May 1993.

46. Ibid.

47. Barlow, "Decrypting the Puzzle Palace," 27. Lotus Notes software is an example of a product produced in two version because of export restrictions.

48. Department of Engineering and Public Policy, *An Assessment of Civil Sector Uses of Digital Data Encryption* (Pittsburgh: Carnegie-Mellon University, November 1980), 2, as quoted in Ferguson, *Private Locks, Public Keys*, 44-45.

49. National Research Council, *Computers at Risk*, 158.

50. J. Laurent Scharff and Jack E. Thomas, "The First Amendment—National Security," in *The First Amendment—The Challenge of New Technology*, edited by Sig Mickelson (N.Y.: Preager, 1989), 67.

51. Ibid., 64.

52. Ibid.

53. William J. Broad, "A U.S. Spy Satellite May Be Sold Abroad," *New York Times*, Nov. 17, 1992, C2.

54. Vincent Kiernan and Andrew Lawler, "Emirates Want to Buy U.S. Spy Satellite," *Space News*, Nov. 16, 1992, 1.

55. J. Laurent Scharff and Jack E. Thomas, *The First Amendment—National Security*, 64.

56. Ibid., 69.

57. William J. Broad, "3 Nations Seek to Buy Spy Satellites, Causing a Policy Rift in U.S.," *New York Times International*, Nov. 23, 1992, A7.

58. Ruth Sinai, "US May Sell Spy Satellite to Gulf State," *Boston Globe*, Nov. 17, 1992, 16.

59. Broad, "3 Nations Seek to Buy Spy Satellites," A7.

60. Ibid., C2.

61. Kiernan and Lawler, "Emirates Want to Buy U.S. Spy Satellite," 1.

62. Ibid., 1.

63. Interview by the author with James Fitzgibbon, Lockheed Corporation, Dec. 9, 1992.

64. Broad, "3 Nations Seek to Buy Spy Satellites," A7.

65. Jeffery T. Richelson, *United States Reconnaissance: Photographic/Imaging Satellites*, ACIS Working Paper, Center for International and Strategic Affairs, UCLA, May 1983, 9,15.

66. Ibid., Table 2.

67. Kiernan and Lawler, "Emirates Want to Buy U.S. Spy Satellite," 1.

68. Interview with Larry Cox.

69. "Sen. Rockefeller Blasts Administration for Winking at Chinese Launch Service 'Dumping,'" *Telecommunications Reports* (Oct. 12, 1992), 29.

70. Interview by the author with Edward Murphy, Department of the Treasury, Office of Economic Policy, Jan. 27, 1993.

Chapter Seven

Technology Transfer

7.1 Technology Transfer Mechanisms

The complex issue of technology transfer does not lend itself to a clear cost and benefit analysis. Access to technology provides the benefits gained from use of the technology and insight into its workings, which promotes its duplication or extension. Diffusion—the process of gaining technological insight—requires careful planning. Simple access to the technology embedded in commercial products usually does not provide the information necessary to duplicate the technology, although export control regulations often miss this point. Because of these confusions, the 1976 Bucy report tried to reorient export control toward processes instead of products. Authorized diffusion, even when complete knowledge of the underlying technology is made available and the developers are cooperative, is difficult and often does not work. The defense industries provide many examples of failures by companies to convert their defense technology into commercial products. The exact type and amount of knowledge necessary for diffusion differs for each technology, making a priori determination of either the damage or benefit from technology transfer very difficult. Arguments about the economic benefits or the national security costs of the transfer of specific technologies or those provided by a protection mechanism need careful consideration.

Chapters Five and **Six** focussed on the problem of technology transfer when an adversary has access to the embedded technology but no other knowledge about it. Circumstantial evidence suggests that, in many cases, access to an embedded technology was insufficient for permanent technology transfer, i.e., damage was restricted to the use made of the specific product the adversary had acquired. Despite strong export control regulations, the Soviets had access—through espionage, diversion, or legitimate purchase[1]—to many of the free world's high-technology products and much of its scientific knowledge, yet they were unable to exploit this access effectively themselves to manufacture comparable high-technology products, except in limited technical areas. This chapter discusses the policy issues for the case where the recipient has greater technical knowledge than only the product.

Knowledge can be broken down into several forms—codified, tacit, or protected[2]— with different characteristics of technology transfer for each form. Codified knowledge is knowledge reduced to general principles so that any properly trained person can understand the information, as in reference books, scientific journals, patents, technical documents, documented experimental methods and techniques, and training courses. Codified knowledge is readily transferrable, because it is well understood and all the relevant information can be put in writing. Tacit knowledge is knowledge based on experience that cannot be written or even stated in easily understood principles, for example, the subtleties of a manufacturing process or directions and techniques for research. Tacit knowledge is not easily diffused, because it relies on the nonquantitative, nonverbal knowledge of individuals.[3]

The different types of knowledge are important, because the relative costs and benefits of technology transfer are subject to the ease with which it can be diffused and used, commercially or militarily. Owing to its highly accessible form, codified knowledge, although protected by export control restrictions, cannot be completely controlled. Tacit knowledge, which requires more extensive human interaction, can be more easily controlled through government regulation, but total control of tacit transfer of defense technology for national security reasons would have an adverse impact on the economic development of defense industries. Any policy must be based on realistic tradeoffs between economic growth and national security.

7.2 Foreign Direct Investment (FDI)[4]

With the dominance of high technology, both dual use and military, by a relatively small number of multinational corporations, the potential for technology transfer of national security information between U.S companies and other countries is increasing. Among the most prominent ways to transfer dual-use technology, especially tacit knowledge, are multicompany alliances,[5] research consortia, joint bidding on contracts, licensing, or outright purchase by one company of another. Most such transfer mechanisms present no new policy questions, because they do not directly transfer critical defense technology outside U.S. national security controls. International alliances and consortia, although they offer possible problems of national security through significant transfer of dual-use technology, are used primarily for commercial technology and therefore do not fall within the boundaries of most U.S. secrecy regulations. Internal alliances and joint military ventures also fall outside U.S. national

security controls. In contrast, FDI, which can remove military technology from U.S. security controls, presents new policy issues.

FDI restrictions present philosophical problems to U.S. national security policy. The U.S., as a society, supports the free-market economic theory of open investment, and trade policies, yet is tolerant of limited exceptions for national security. This philosophy is being tested by changing defense needs together with increasing amounts of foreign investment in the U.S. With a declining defense budget, owing to the end of the Cold War, maintaining the current defense base is probably impossible. The difficult choices facing the society include maintaining the industrial base through continuing high defense spending, allowing unnecessary companies to go out of business, or allowing industrial consolidation of both U.S. and foreign firms. Possible benefits of consolidation include the saving of some jobs in the defense industry and maintenance of most of the industrial base. The end result of consolidation, however, fewer defense jobs worldwide,[6] would increase the need for merger of U.S. and international firms.[7] Its danger is that foreign companies might acquire U.S. companies and gain access to U.S. technology while also cutting U.S. jobs. The loss of national security technology through industrial restructuring must be addressed.

Foreign investment has become a sensitive political issue quite apart from arguments specifically about economics and national security. Many factors contribute to increased public sensitivity to foreign investment. First, the 1980s saw a dramatic increase in the amount of foreign investment. Previously, U.S. business had invested heavily outside the country but foreign investment in the U.S. was comparably small. In 1980, the U.S. had $220 billion in foreign investments, yet only $83 billion was invested in the U.S. (both figures reflect direct investment and exclude such investments as Treasury bonds). By 1990, U.S. investments abroad had increased to $421 billion, but inward investment had grown to $404 billion.[8] Such substantially increased investment in so short a time led to fears that foreigners were buying up the best American companies.[9] This sensitivity to foreign investment may be subsiding somewhat. The inward investment figures peaked in 1989 and have dropped since then, partly in response to the worldwide economic downturn.[10] **Table 7-1** provides a breakdown of investment during the 1980s. Second, the rules protecting U.S. business from foreign takeovers were changed. Congress perceived several high-profile sales[11] of important

military technology to foreign companies as weakening national security and consequently passed stronger national security exceptions to investment laws.[12]

Table 7-1

Comparison of Foreign Direct Investment (FDI)

Year	U.S. Investment ($U.S. Billions)	Investment in the U.S. ($U.S. Billions)
1980	215.375	83.046
1985	230.250	184.615
1987	314.307	263.394
1988	335.893	314.754
1989	370.091	373.763
1990	421.494	403.735

Source: U.S. Bureau of the Census, *Statistical Abstract of the United States: 1992* (Washington, D.C., 1992), Table 1319, p. 786, and Table 1324, p. 789.

7.2.1 Benefits of FDI

Public uneasiness with foreign investment notwithstanding, FDI provides many economic and national security benefits, primarily the influx of new capital to shaky U.S. companies. When major defense components are made by just one supplier, the health of that supplier, and consequently the availability of the components, is an important national security concern. The controversial 1992 proposal to acquire LTV by the French company Thomson clearly illustrated this concern. LTV was the principal or sole supplier of missile components—the MLRS multiple rocket launcher, the ERINT antitactical missile interceptor, and the LOSAT antitank missile system,[13] so its survival was a national security interest. When it filed for Chapter 11 bankruptcy, the judge overseeing the proceedings attempted to sell the business.[14] Although the controversy eventually brought about the purchase of LTV by a U.S. defense company,[15] consolidation of the defense industry may rule out such an option in other instances. Foreign investment also contributes to inward technology transfer, either by increased R&D or in the direct transfer from the purchasing company.[16] An example of inward technology flow is the increase in productivity by U.S. manufacturing affiliates of

foreign firms of 40 percent between 1980–87 compared with that by U.S. firms of 32 percent in the same period.[17] The benefits gained from technology transfer may outweigh the national security concerns.

7.2.2 National Security Concerns

Although FDI provides economic benefits, it presents national security concerns in addition to those related to technology transfer, including dependence on foreign suppliers, reduced development of technology in the future, and an eroding manufacturing base. The potential loss of control over sensitive technologies represented by FDI poses two national security concerns: the ability of another country to acquire sensitive technology and to challenge the U.S. and the inability of the U.S. to access technology, thus incurring a loss of U.S. capability. The first concern applies equally to all technology transfer, but the second is unique to FDI. Foreign companies and their subsidiaries are under no obligation or, owing to security regulations of either the U.S. or their own countries[18]—indeed they may not even have the ability—to build U.S. national security equipment. The issue of foreign subsidiaries denying the U.S. the use of technology needs further study, yet history shows that U.S. subsidiaries of foreign firms act very much like U.S. firms[19] and that concern about potential loss of technology has not been valid in the past. If a foreign company were the only supplier of patented technology, the U.S. would only have access to the technology by permission of that company and its government.

Technical dependence is "when the US must acquire advanced technology for critical weapons development from a foreign source."[20] If a foreign country originates a critical technology, preventing dependence may not be possible. The U.S. could develop a situation of dependence on U.S.-originated technology. Foreign investment could also affect future U.S. technology through redirection of R&D, especially critical if the acquired firm were involved in national security R&D. The benefit of R&D would go to the foreign company, not to the U.S., thus creating the potential for dependence. The long-term impact of foreign investment on the overall defense base might be negative. Allowing foreign companies to acquire significant parts of defense industrial sectors, even if technology transfer issues are ignored, could lead to a significantly eroded U.S. industrial base and, again, the potential for dependence.

7.2.3 Investment Restrictions

Because of these concerns over foreign investment in the defense industry, the Committee on Foreign Investment in the U.S. (CFIUS) was set up to review foreign acquisitions with possible impacts on national security. Following a study required by the Foreign Investment Study Act of 1974,[21] in 1975 President Ford set up the CFIUS[22] as a presidential committee. Consisting of the secretaries of Treasury, Defense, State, and Commerce, the Attorney General, the director of the Office of Management and Budget (OMB), the U.S. Trade Representative (USTR) and the chair of the Council of Economic Advisors, the CFIUS was charged with overseeing the foreign investment process. In 1987, during debate of the Fairchild-Fujitsu merger, weaknesses in the existing law were discovered that made prevention of an acquisition extremely difficult. The president had to invoke the IEEPA and declare a national emergency to stop the acquisition.[23] The Exon-Florio amendment to the 1988 Omnibus Trade and Competitiveness Act, which institutionalized the CFIUS committee, gave the president authority to block foreign acquisitions. On December 28, 1988, by executive order,[24] the Secretary of the Treasury, as chair of the CFIUS, was given the responsibility for reviewing foreign investment proposals.

Exon-Florio allows the president to block foreign acquisitions if:

> 1. There is credible evidence that leads the President to believe that the foreign interest exercising control might take action that threatens to impair the national security; and
>
> 2. Provisions of law, other than this section and the International Emergency Economic Powers Act, do not in the President's judgement provide adequate and appropriate authority for the President to protect the national security in the matter before the President.[25]

The president was required to consider three factors in the decision.

> 1. Domestics production needed for national defense requirements
>
> 2. The capability and capacity of domestic industry to meet national defense requirements
>
> 3. The control of domestic industries and commercial activities by foreign citizens as it affects the capability and capacity of the United States to meet the requirements of national security.[26]

In 1992, to reflect post-Cold War interests, Exon-Florio was modified[27] to include two additional factors the president must consider:

> 1. The potential effects. . .on sales of military goods, equipment of technology to any country supporting terrorism and any country of concern regarding the proliferation of nuclear technology, missiles, or chemical and biological weapons
>
> 2. The potential effects of the proposed or pending transaction on U.S. international technology leadership in areas affecting U.S. national security[28].

The review process consists of an interagency review by the eight statutory agencies and any others invited by Treasury. Each proposal undergoes an initial thirty-day review for national security implications. If no concerns are discovered, the process is concluded. If possible national security concerns are discovered, a forty-five day, in-depth review is conducted. Following the second review, the president has fifteen days in which to make a decision.[29] Each agency reviews the proposal from the standpoint of its own mission, with consideration by the committee of the economic and national security tradeoffs. For example, the DOD assesses risks involved in technology transfer, the possible effect of the proposal on the U.S. defense base, and on defense contracts, including their scope and contractual provisions.[30]

As of November 1, 1992, the CFIUS had conducted 751 reviews. Fifteen transactions required the formal forty-five day review, with the rest approved after initial review. The president prohibited one transaction, chose not to intervene in another nine, and the remaining five were withdrawn.[31] Although the CFIUS committee does not recommend disapproval of many acquisitions, a major benefit of its review might be to prevent transactions with potentially serious national security concerns from even being proposed because companies know the proposed acquisition will be rejected.

Signalling a possible change in philosophy from that of his predecessor, President Clinton has announced a review of the sale of the Applied Magnetics Corporation, maker of components for laser disk drives, to Nakamichi Peripherals, Inc., which had been approved by President Bush on his last day in office.[32] The national security concern was that Applied Magnetics was the only U.S. producer of the laser disk drives used in both the Trident and Patriot missiles.[33]

Business leaders interviewed for this study were generally satisfied that the CFIUS process strikes an acceptable balance between national security and economic concerns. It leaves leeway for judgement and common sense, while eliminating those few acquisitions that offer major national security concerns. But the same leaders felt that the U.S. must avoid the danger of unconstrained protectionism on investment, which could result in damaging global retaliation against the operation of U.S. companies abroad.[34]

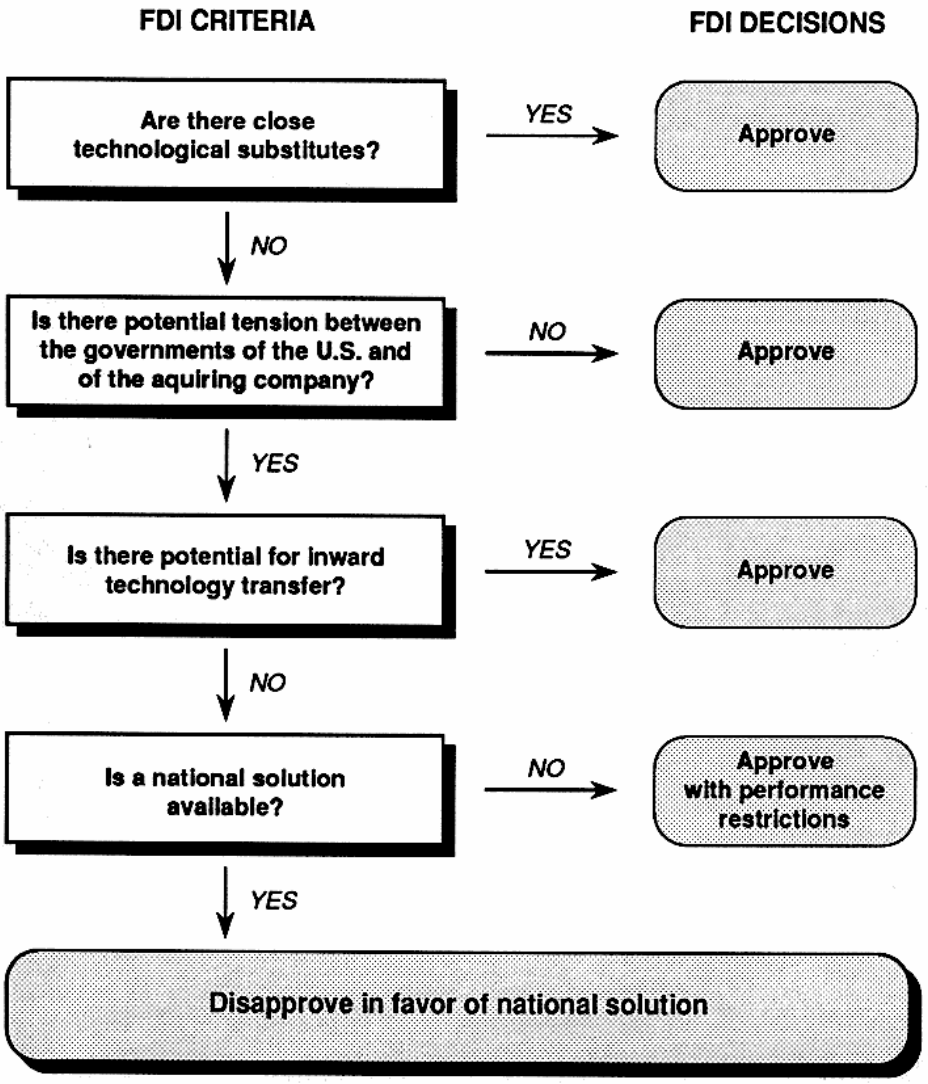
There are other, less direct methods to guard against technology transfer than the CFIUS process. Because FDI has both economic and national security implications, changes in economic climate can make foreign investment unattractive. Techniques that governments can manipulate to protect against foreign investment include:

- ownership regulations
- taxes or subsidies, or both
- currency regulations
- price controls
- sector-specific incentives and limitations
- application and entry procedures
- performance controls.[35]

Performance restrictions, although not formally part of the CFIUS process,[36] have an important role in the protection of technology. One common restriction involves developing a management structure that inserts Americans between the technology and the foreign owners. U.S. managers can ensure that the technology is protected according to applicable classification or export control regulations. Other performance controls include: export control regulations, clearance regulations, facility clearance requirements, and requirements for bidding on defense contracts. By shielding national security technology from foreign owners, performance restrictions allow economic improvements, such as needed capital or innovative management techniques, without the corresponding costs of technology transfer. Opinions in government and industry differ, however, about whether these performance restrictions afford real protection of technology.[37]

7.2.4 Foreign Investment Model

A possible model of a strategy for foreign investment developed by Theodore Moran, and outlined in **Figure 7-1**,[38] requires the acquiring company to show that the acquisition serves



Source: Adapted from Theodore H. Moran, *American Economic Policy and National Security* (N.Y.: Council on Foreign Relations, 1993), 57.

Figure 7-1

FDI Decision Tree

the national security interest of the U.S. It defines several factors the policymaker must consider before allowing the acquisition, including the following:

- the number of close substitutes for the disputed technology (because more substitutes mean less chance of dependence);

- the relationship between the U.S. and the government of the acquiring company (because fewer potential conflicts between governments mean less chance that the company might deny the U.S. access to the technology);

- the technology level of the acquiring company (because a more advanced acquiring company is less liable to be buying the company for its technology);

- the availability of a domestic solution with the same economic advantages.

If problems were to remain, the government could impose a national solution, by subsidizing the company to guarantee a domestic base or by imposing performance requirements on the acquiring company and its subsidiary to ensure U.S. national interests.

Applying his model to the LTV-Thomson proposal, Moran concluded that the acquisition should have been rejected on national security grounds. LTV had few substitutes for its missile product line; the potential for conflict existed between France and the U.S. over national security issues; Thomson brought no technology strengths that would help LTV; and a potential domestic solution was available from other U.S. defense firms. Moran concluded that the national solution was better than the acquisition even with performance restrictions.[39]

7.3 Defense Conversion

Irrespective of the problems in technology transfer, the government actively encourages the transfer of government-developed defense technology to the U.S. private sector in order to promote economic competitiveness. Even though the technology is unclassified, defense conversion raises questions of national security because of the need to protect much of the technology against further transfer. The techniques used to encourage defense conversion include increasing the access of industry to existing mission-oriented technology, joint government-industry R&D, easing patent restrictions on government technology, allowing industry to use government facilities and hire government employees as consultants,[40] and reviewing the classification requirements of technology.

7.3.1 Government Incentives

Defense technology plays a large role in U.S. R&D and has the potential for a large economic impact. The national security community, including the defense portion of the

Department of Energy (DOE), will spend approximately $42 billion and account for 59 percent of federal R&D in 1993.[41] Although defense cuts may reduce these totals slightly, defense R&D will continue to provide a large percentage of overall U.S. technological development. Much of this research is conducted in 726 federal laboratories, including three large DOE labs, Livermore, Sandia, and Los Alamos.[42] In his technology plan President Clinton announced that he wants all DOE, National Aeronautics and Space Administration (NASA), and DOD laboratories to promote technology transfer by devoting at least 10 to 20 percent of their budgets to R&D partnerships with industry.[43]

Commercial use of federal technology, even when freely available, is not automatic.[44] Because national security technology develops from different pressures, commercialization usually requires additional effort by industry. Technology developed for the military often does not meet industrial unit cost or commodity manufacturing requirements. Prior to 1980, federal-to-commercial technology transfer was minimal, because there was little or no incentive for industry to spend the necessary time and money to commercialize defense technology.

Congress has long been interested in technology transfer. The 1980 Stevenson-Wydler Technology Innovation Act gave the federal government an explicit transfer mission by recognizing the "responsibility of the Federal Government to ensure full use of the results of the Nation's Federal investment in research and development."[45] The mechanisms developed by the bill were not fully implemented by the Reagan administration.[46] The Bayh-Dole Act of 1980 modified the patent law to allow federal agencies to grant exclusive licensees to private parties and gave small business, university, and nonprofit organizations the right to patents for technology developed on government contracts. Restrictions remain for defense contractors that require the government investment to be reimbursed before the liberalized patent rules take effect. This response to this Act was disappointing. In 1990, federal licensing royalties totalled only $9.4 million.[47] The Federal Technology Transfer Act of 1986 established Cooperative Research and Development Agreements (CRADA) that permit joint ventures. The National Competitiveness Technology Transfer Act of 1989 extended CRADAs to national weapons laboratories, such as Sandia. At the end of 1992, the DOE laboratories were the most active in technology transfer ventures, with more than 250 CRADAs worth more than $300 million.[48]

7.3.2 Issues

In the general enthusiasm of both industry and the government to promote the economic benefits of defense conversion, national security considerations must still be respected. The discussion of technology transfer in **Chapters Five** and **Six** showed that the U.S. goes to great lengths to protect "sensitive" unclassified technology and information. These considerations do not disappear when the government is the originator of the technology. Among the policy issues that need to be addressed are the following:

- How to determine what technology to transfer
- The qualifications of the intended recipients of the technology
- The process for transferring the technology
- The end-use restrictions on the technology
- How to protect technology not being transferred
- Means to enforce the restrictions
- Ramifications on defense procurement
- Transfer between the defense and the commercial departments of defense contractors

Not all unclassified government technology is suitable for transfer to industry. Some is not commercializable, because it does not meet a commercial need, the transfer process is too hard, the resultant product cannot be manufactured at reasonable commercial costs, or has national security sensitivities. Who—government or industry—decides which technology to transfer is an important policy question. The government, with little experience or knowledge of industry requirements or of potential markets, would be highly inefficient in picking technologies to commercialize. Industry, even though more efficient in determining possibilities for commercialization, would need access to all available technology to decide which to transfer. Because industry is not a monolith but made up of innumerable individual companies interested in different technologies, letting it decide would be inefficient and would widely expose "sensitive" technology.

Just as important as which technology to transfer is identification of its recipients. The policy issues discussed in regard to FDI also apply here. Another goal of President Clinton is to move the DOD toward greater use of commercial products and away from reliance on internal development.[49] A wrong decision on which company should receive the technology

might foster technical dependence. Although national security arguments may lead to the conclusion that only U.S. companies should be eligible, economic considerations point toward more open transfer. Because technology transfer usually is an inexact and costly endeavor, the potential for commercialization differs by company. For example, considerations such as those related to technology experience or distribution chains might make commercialization more valuable to a foreign company than to a U.S. one. The effect of restrictive eligibility requirements might be the sacrifice of economic benefits by the government, both to itself in licensing fees and to the U.S. consumer in the form of better products.

Technology and information that is not supposed to be transferred, such as related classified technology, must be protected during transfer. Transfer can occur through consulting agreements, licensing, personnel exchange, access to facilities, access to embedded technology, CRADAs, or written material. The actual process must be carefully set up to ensure that access is limited to the specific technology and so that related material can be protected. Information that might be relevant to commercialization but must still be protected include its specific national security use, technological improvements, related technologies, and the manufacturing process. One example of this problem is commercialization of photographic satellites (discussed in **Chapter Six**).

Once the technology has been transferred, the commercial products developed from it may need end-use restrictions, such as export control. While the advisability of transfer is under determination, the government must examine the need for and the potential effectiveness of end-use restrictions to protect the technology. Transfer may not present any concerns if restrictions can be effectively imposed, or the commercialization time lag may preclude the need for restrictions, or for compensating reasons further transfer of the technology through a commercial product is not possible. If end-use restrictions will not be effective, the policy needs to indicate whether the economic benefits of the technology outweigh the probability of further transfer.

National security technology is not limited to the government. Defense contractors also maintain defense technology, especially the manufacturing techniques used to produce much of the high technology. Some of this internal knowledge might be useful in the commercial divisions and does not transfer sensitive technology. Because most large defense contractors

are also large commercial developers,[50] for which defense contracts may be less than 10 percent of their total sales, the economic benefits of internal business technology transfer could be large. The present regulations do not address this facet of technology transfer, but focus instead on government-to-industry. A major stumbling block to this intracompany transfer is defense procurement rules that encourage companies to segregate commercial from defense production, which eliminates many avenues for technology transfer. Among the factors that cause such segregation are the different accounting systems imposed on defense procurement,[51] technological divergence, conflicts in goals, patterns of production and use, requirements on government procurement, and different cost philosophies.[52] By encouraging closer interaction between defense and commercial divisions, the government could accomplish some of its technology transfer objectives.

7.4 Foreign Military Sales

Beyond the transfer of government technology to U.S. commercial firms, the government also sanctions the transfer of national security technology, classified and unclassified, to foreign governments through the Foreign Military Sales (FMS) program. Foreign sales are a lucrative part of the defense industry: between 1990–92 they totaled $54 billion, and the Pentagon projects 1993 sales at another $30 billion, half through the FMS program.[53] The consequences of these sales, justified on geopolitical, national security, and economic grounds, raise many policy questions. The FMS policy must define which technology to sell, what qualifications a purchaser must have, what end-use restriction should be placed on the technology, how to enforce them, and the economic considerations.

Through FMS, the U.S. sells some of the most sophisticated technology the country possesses,[54] along with the training necessary to facilitate its use. During the Cold War the primary rationale for the sales was to support western military interests. The countries being sold the technology were determined by national security considerations based on the East-West hot spots, adjusted by political considerations. Four primary criteria must be taken into official consideration in the decision process:

- Consistency with U.S. foreign policy
- Effect of the sale on U.S. national security
- Ability to impose and enforce necessary end-use controls

- Quid pro quo from the receiving country[55]

Although these criteria do not include economics, the economic benefits of FMS are obvious, primarily the use of foreign sales in maintaining the defense industrial base, recovering research and development costs, while also providing political and military support for U.S. allies. Many groups within the Services, in particular operations and logistics, push for increased FMS as a means to strengthen the industrial base.[56]

Because determination of which technology can be sold to which countries is ambiguously grounded in identifiable national security objectives, it has taken on political overtones. Although very sophisticated technology is being sold, limitations are still necessary to ensure that the U.S. maintains a technological lead over the rest of the world. One result is that products, such as tanks and planes, are sold fairly easily while information, such as software and manufacturing knowledge, is seldom sold.[57] Given the recent large increase in FMS[58] and the absence of any articulated post-Cold War FMS policy, the tradeoffs appear to be tipping toward economic competitiveness and away from national security.

Possible problems with FMS include use of the technology by the recipient against the U.S., duplication of the technology, or its reexport to another country. Although export control restrictions on end use, such as inspections or setting limits on acquisition of spare parts, may help to alleviate some of the problems, they appear inadequate protection against *all* potential problems. Additional safeguards against transfer may be necessary for critical technology. These considerations form part of the decision of the level of technology allowed to be sold through arms exports.

Notes

1. *Balancing the National Interest*, 51.

2. Alic et al., *Beyond Spinoff*, 28-34.

3. Ibid., Table 2-1, 30.

4. The International Investment Survey Act of 1976, 22 USC 3101-3108, defines direct investment as "ownership or control, directly or indirectly, by one person of 10 percent or more of the voting securities of a corporation or the equivalent interest of a non-incorporated enterprise" (cited in Gauger, et al., *US National Economic Security in a Global Market*, 17).

5. "When Multinationals Marry," *The Economist*, Sept. 19-25, 1992, 19.

6. Martin Dickson, "Ending of Cold War Hots Up a Merger," *London Financial Times*, November 24, 1992, 23.

7. Two examples of consolidation in the defense industries are the acquisitions of the military-aircraft business of General Dynamics by Lockheed in December 1992 and of General Electric Aerospace by Martin Marietta in November 1992.

8. Department of Commerce, *Statistical Abstract of the United States 1990*, Table 1319, page 786 and Table 1324, 789.

9. John Bryant's statement to the House Subcommittee on International Economic Policy and Trade in 1988 summed up the fears of most Americans over foreign investment: "Foreign investment in the United States represents an economic invasion more dangerous than any we have experienced in our history. It threatens to turn us into a nation of stewards and servants. Foreign investors are buying our productive assets as a means of controlling us politically as well as economically. They are pirating our most advanced technology and undermining our national security" (cited by Gauger et al. from Defense Public Advisory Committee on Trade [DPACT], *Foreign Ownership of Defense Related Industries*, Issue Paper, Sept. 2, 1989, cited by Gauger et al. in *US National Economic Security in a Global Market*, 34).

10. In 1989, FDI was $60 billion, which decreased to $30 billion in 1990 and further to $15 billion in 1991. Edward M. Graham, "Foreign Direct Investment in the United States and U.S. Interests," *Science*, Dec. 20, 1991, Fig. 1, 254. According to the unpublished Commerce Department document, "Implementing Exon-Florio," foreign investment continued to fall in 1992.

11. Among them were the FSX venture with Mitsubishi, the proposed sale of Perkin-Elmer to Nikon, and the sale of Fairchild to Fujitsu. Susan Tolchin, "U.S. Moves to Guard Vital Industries," *Defense News*, Oct. 19, 1992, 27.

12. §5021 (Exon-Florio) of the Omnibus Trade and Competitiveness Act of 1988 (§721 of the Defense Production Act). PL 102-99, Aug. 17, 1991, made §721 permanent, exempting it from the requirement of periodic renewal as part of the Defense Production Act.

13. Theodore H. Moran, *American Economic Policy and National Security* (N.Y.: Council on Foreign Relations, 1993), 58.

14. Bureau of National Affairs, "Thomson Bid to Acquire LTV Continues to Generate Fallout in Congress, Court," *Daily Report for Executives*, Sept. 29, 1992 [NEXIS.]

15. "Thomson Bid to Acquire LTV Continues to Generate Fallout in Congress, Courts." LTV was bought by a consortium consisting of the Loral Corp., the Carlyle Group, and Northrup.

16. Sumiye Okubo McGuire, "Summary and Conclusions," in Department of Commerce, *Foreign Direct Investment in the United States*, 86. The Department of Commerce reports that license and royalty fees paid by U.S. affiliates increased rapidly, suggesting an inward flow of knowledge from the parent company. It also reports that in 1987, the U.S. affiliates spent 7.6 percent on R&D, while U.S. firms spent 6.5 percent.

17. Ibid., 86.

18. Foreign Ownership, Control, or Influence (FOCI) rules limit what foreign owned companies can provide for U.S. military contracts. According to Gauger et al., in *US National Economic Security in a Global Market*, (25): "Investigations are conducted by contractors seeking classified contracts and any firms found to be under foreign ownership, control, or influence (FOCI) are not eligible for a clearance. The determination of FOCI is a subjective analysis that consists of evaluating the following factors:

1. Is there foreign direct or beneficial ownership of five percent or more of a firm's securities?
2. To what extent do foreign interests hold management positions or control or influence directors, officers, or executives of an organization?
3. What is the extent of a company's contracts with or indebtedness to foreign interests?
4. Does it have income from foreign interests that exceeds 10 percent of its gross income?
5. Is there any other evidence indicating the capability of a foreign interest to control or influence management or operations in order to obtain access to sensitive information."

(Cited by Gauger et al. from Mark L. Hanson, "The Regulations of Foreign Direct Investment in the United States Defense Industry," *Northwestern Journal of International Law and Business* (1989), 666.)

19. McGuire, "Summary and Conclusions," 86.

20. Gauger et al., *US National Economic Security in a Global Market*, 57.

21. Foreign Investment and Survey Act of 1976, PL 94-472, 22 U.S.C. §3101-3108.

22. Gauger et al., *US National Economic Security in a Global Market*, 27.

23. Ibid., 28-29.

24. Unpublished document, Department of Commerce, *Implementing Exon-Florio*.

25. Ibid. Exon-Florio Amendment, §5201 of the Omnibus Trade and Competitiveness Act of 1988, PL 100-418. On Aug. 17, 1991, PL 102-99 made Exon-Florio permanent, replacing the provision for periodic reauthorization.

26. Lucinda Low, "Amendments to Exon-Florio Law: Foreign Investment in U.S. National Security Businesses," *National Security Law Report*, **15**, 4 (April 1993), 2.

27. National Defense Authorization Act for Fiscal Year 1993, PL 102-484.

28. Ibid.

29. Unpublished document, Department of Commerce, *Implementing Exon-Florio*.

30. Interview with George Menas.

31. Unpublished document, Department of Commerce, *Implementation of Exon-Florio*.

32. Keith Bradsher, "U.S. Seeks to Reopen Japan Deal," *The New York Times*, Jan. 26, 1993, D1.

33. "The National Security Agenda," *National Security Law Report*, **15**, 5 (May 1993), 6.

34. Interview by the author with Jonathan Huneke, U.S. Council for International Business (USCIB), Feb. 8, 1993.

35. United Nations Centre on Transnational Corporations, *Government Policies and Foreign Direct Investment* (N.Y.: UNCTC Current Studies, Series A, No. 17, November 1991).

36. Interview with George Menas. Performance restrictions are handled outside the CFIUS process by the Defense Industrial Security Agency. The CFIUS uses the restrictions, if any, as input to their final recommendation.

37. Knowledgeable people are easy to find on either side of the issue. For example, according to Huneke (see note 34), evidence suggests that the current performance restrictions have been adequate to protect the technology. Fred Demech, TRW (interview with the author, Dec. 11, 1992), has said that the restrictions are not strong enough to protect technology. Unfortunately, at present little empirical data exists to support either conclusion.

38. Moran, *American Economic Policy and National Security*, 57.

39. Ibid., 58-59.

40. Ronald E. Yates, "Refitting Cold War Science," *Chicago Tribune*, Oct. 26, 1992, IV-1.

41. President William J. Clinton and Vice President Albert Gore, Jr., *Technology for America's Economic Growth: A New Direction to Build Economic Strength*, Washington, D.C., Feb. 22, 1993, 8.

42. Yates, "Refitting Cold War Science," IV-1.

43. *Technology for America's Economic Growth*, 9.

44. This history of technology transfer is based on the discussion in Alic et al., *Beyond Spinoff*, 76-79.

45. Cited in *Beyond Spinoff*, 77.

46. Ibid., 77-78

47. John R. Emshwiller, "Collegians at Federal Labs Major in Commercialization," *The Wall Street Journal*, Sept. 17, 1992, B2.

48. Barry M. Daniel, "Technology Transfer—A National Energy Imperative," *Aerospace Industries Association Newsletter*, December 1992, **5**, 6, 1.

49. *Technology For America's Economic Growth*, 4.

50. *Beyond Spinoff*, Table 6-A-1, 192.

51. Interviews by the author with Charles Tringali, Lockheed, Dec. 9, 1992, and with Fred Demech (see note 37).

52. *Beyond Spinoff*, 144-153.

53. Aaron Zitner, "Arms Across the Sea," *The Boston Globe*, Aug. 1, 1993.

54. In the latest examples, the U.S. agreed to sell 150 F-15s to Taiwan and seventy-two F-16s to Saudi Arabia in the fall of 1992; "F-16s in 4 European Countries to be Upgraded," *Central News Agency*, Oct. 30, 1992.

55. Interview by the author with Fred Mannke, Department of the Army, April 28, 1993.

56. Ibid.

57. Ibid.

58. The effectiveness of U.S. weapons in Desert Storm and the pressures on defense industries in reducing defense budgets caused FMS to jump in 1991.

Chapter Eight

Civil Liberties

> Perhaps it is a universal truth that the loss of liberty at home is to be charged to provisions against dangers, real or pretended, abroad.
>
> James Madison[1]

8.1 Overview

Secrecy represents more than a process of limiting access to selected information and technology; it also embodies a value system that illustrates an unwritten agreement between the public and the government about the relative importance of security and individual rights. Although this study has looked at secrecy policy primarily from the perspective of economic competitiveness and national security, equally if not more important tradeoffs are concerned with the proper balance of national security and civil liberties. These tradeoffs, many related to fundamental constitutional tensions, appear in critical policy areas. This chapter examines secrecy from the point of view of individual rights.

Constitutional arguments, which balance conflicting but fundamental rights, usually do not have a clear, consensual answer but more often reflect the mood of the public, politicians, and government institutions at the time. Executive privilege, which balances the need of the executive branch to keep some activities secret and the need of the public for disclosure (through Congress), has been a contentious political issue in recent years. Prior restraint on publication, in the media and in academia, balances the First Amendment right of free speech with national security needs. Law enforcement information presents many of the same problems as national security because of the overriding importance of public safety. Privacy from unnecessary government intrusion and knowledge of government actions, which are fundamental rights, conflict in the Freedom of Information Act and the Privacy Act. Privacy, like national security, requires that large amounts of government information must be protected.

The resolutions of these tensions affect the amount and type of information citizens hold about both the government and one another. These tensions raise questions about the importance society places on its basic ideals as opposed to compromises of those ideals that

may be politically necessary to survive in today's world. Given strongly held feelings about these issues, the resolutions are not permanent but change with the sense of danger felt by society and the perceived need to compromise principles, such as civil liberties, for reasons of security.

8.2 Executive Privilege

Executive privilege, like classification, is another Cold War battlefield over control of information. Prior to World War II, the doctrine of executive privilege was a constitutionally vague, but relatively minor, issue.[2] Presidents since Washington have maintained that in limited cases the president's need to limit disclosure of information in order to conduct the business of the office outweighs the public's right to government information. Conflicts between the president and Congress normally were resolved through negotiation, rarely reaching the point of the invocation of privilege. During the Cold War, however, executive privilege became significant, both in the number of times it was invoked and in the ensuing controversies. Although executive privilege is seldom formally invoked, the refusal by administration witnesses to testify or the withholding of requested information without invocation of executive privilege has become fairly common.[3] Two recent high-profile cases were Watergate and Iran-Contra, in both of which political grandstanding tended to obscure the underlying constitutional issues involved in the denial of information to Congress by the executive branch.

8.2.1 History of Executive Privilege

In 1941, Attorney General Robert Jackson started the modern argument about executive privilege by refusing to comply with a House request for files of the Federal Bureau of Investigation (FBI).[4] In 1954, in response to perceived Congressional abuses during the McCarthy hearings, President Eisenhower prohibited Defense Secretary Wilson and his subordinates from testifying before Congress.[5] In 1958, Attorney General William Rogers[6] claimed that the president has the discretion to withhold from Congress *any* information about the executive branch, including testimony by current and former federal employees.[7] Congress, charged with overseeing the executive branch, asserts that it must have the ability to force the executive to provide the information Congress needs to fulfill its oversight responsibilities. Executive privilege raises two competing constitutional questions: first, can the president bypass the checks and balances of Congress by selectively sharing and

withholding information from it and, second, do Congressional demands for access to executive information violate the separation of powers doctrine. The answers to these questions, continually redefined by political pressures, have moved beyond the strictly legal and have to be found in the arenas of politics and ethics.

Historically, executive privilege[8] has rested on the doctrine of the separation of powers, that is, the balance of the legislative function of Congress and the executive's duty to execute the law.[9] That the legislative function of Congress includes the ability to compel testimony about actions of executive branch has a long history, having been adopted from the right of the English Parliament to investigate the King. Precedents from the 1600s[10] show that Parliament could examine documents and call witnesses during an investigation, even royal advisors.[11] Comparable powers for the Colonial legislators were demonstrated by legislative inquiries in Massachusetts in 1722 and in Pennsylvania in 1770. The courts accepted the historic concept of investigation in McGrain v. Daugherty:

> The power of inquiry—with the power to enforce it—is an essential and appropriate auxiliary to the legislative function. It was so regarded and employed in American legislatures before the Constitution was framed and ratified.[12]

The Constitution, which delineated the functions of both Congress and the president, was written with this history in mind. The Constitution says nothing about the legislative need for, or ability to compel, executive information. Advocates of both sides have used this omission in their arguments. Opponents of an expansive executive privilege argue that the Constitution did not explicitly define legislative investigative powers, because the right was already firmly rooted. Proponents of the privilege say that the framers of the Constitution denied Congress the ability by not explicitly granting it the right of access to executive information.

History shows that the first presidents did not make sweeping claims of executive privilege. Washington denied only one Congressional request for information. In 1792 his cabinet agreed that they could refuse to supply information to Congress if injurious to the public but never claimed executive privilege and eventually turned over the disputed information. In 1796, Washington refused a House request for information concerning the Jay treaty on the grounds that the Senate, which reviews treaties, had already received the information. Congress, however, pressed its claim for the right to examine executive branch

information. It inserted a provision in the 1789 bill establishing the Treasury Department[13] that required the Secretary of Treasury to report any information that Congress requests that pertains to that office.[14] No such provisions were added when the department of State and War were established. As with the wording of the Constitution, each side claims that these omissions support its own arguments.[15] Provisions requiring disclosure of information to Congress were enacted for 127 other agencies and organizations before a general provision was enacted in 1928[16] that requires disclosure by all federal agencies.

The underlying constitutional issue was avoided in the early years legislative acceptance of presidential discretion. Jefferson and Monroe were granted permission by Congress to provide information "except such as he may deem the public welfare to require not be disclosed"[17] in specific disagreements over information. The first instance of executive refusal to provide information without prior permission was in 1835 by Jackson. The second use of executive privilege was in 1843 by Tyler. Early presidents, although supportive of the concept of executive privilege, appeared to consider the concept limited and were reluctant to invoke it.[18]

The Constitution gives the president the responsibility to execute the laws of the U.S. and to be the Commander in Chief of the military. Executive secrecy against Congress and, by extension, the public has been asserted by presidents as necessary to fulfill these functions. A 1958 memorandum from Attorney General Rogers identified five areas of privileged disclosure:

1. military and diplomatic secrets and foreign affairs;
2. information made confidential by statute;
3. investigations relating to pending litigation, and investigative files and reports;
4. information relating to internal government affairs privileged from disclosure in the public interest; and
5. records incidental to the making of policy, including interdepartmental memoranda, advisory opinions, recommendations of subordinates and information working papers.[19]

Rogers claimed, and his claim was later supported by Attorney General Kleindienst during Watergate, that protection from disclosure extended to all federal employees on the basis of their role as extensions of the president. The president had the right to refuse any executive

branch information, on the grounds solely of presidential determination of the public interest, without judicial review.

8.2.2 Issues

The president's need for secrecy from Congress and the public is based not on national security but on the independence of the executive as a separate, co-equal branch of the government. According to Richard Kleindienst in testimony before Congress:

> If another branch of Government could compel the attendance of the President, for the purposes of inquiring into the performance of his official duties, it would seriously impair the independence of the Presidency and the executive branch. . . . [President Truman stated that] If a President or former President could thus be called and questioned about his official duties, "the office of President would be dominated by the Congress and the President might become a mere appendage of Congress."[20]

Recognition of the need for executive secrecy comes from both congressional and judicial sources. Congress, in legislation, agreed that the public interest allowed the executive branch to withhold certain information from public access. For example, the FOIA provides exceptions from public release for all categories of information identified in Attorney General Rogers' memorandum. The Supreme Court in the case of the Nixon Watergate tapes[21] acknowledged that the president had a presumptive right to protect information, such as national security, foreign policy, and private communication, from the other branches of government,[22] but the Court found that this right can be outweighed and the president forced to release information if that information is necessary to fulfill other constitutional requirements.*****

Congressional arguments against unlimited executive secrecy assume that Congress represents the public in acting to ensure that executive departments operate correctly. The constitutional tools necessary for oversight arise from its duties of appropriating money, legislation, and impeachment, each of which requires access to executive branch information that the president might be reluctant to provide.

*****Other judicial opinions that uphold portions of executive privilege include United States v. Curtiss-Wright Corporation (299 U.S. 304, 320 [1936]), United States v. Reynolds (345 U.S. 1 [1953]), and Soucie v. David (448 F. 2nd 1067 [D.C. Circuit 1971]).

The executive agencies hold a monopoly on information that concerns execution of the laws. Neither Congress nor the judiciary can oversee executive agencies without the president's cooperation in providing appropriate information. The president can effectively prevent informed debate on any legislative initiative by refusing to cooperate with Congress or its supporting institutions, such as the General Accounting Office (GAO). Unlimited discretion, even if constitutional, allows the president to stonewall any investigation into the actions of the executive branch, as was alleged in the Iran-Contra investigation. Congress is not defenseless—its political powers range from legislative and appropriations control over executive programs to legal remedies such as impeachment and citations for contempt of Congress[23]—and although its powers cannot force a president to turn over information, Congress can raise enough political trouble that a president may be willing to negotiate with it. In test cases of the general issue of "withholding" information from Congress during Iran-Contra, prosecutions for withholding information and even willfully lying to Congress were generally unsuccessful.

Protection of classified information, the primary justification for secrecy, is not a major issue in executive privilege, because Congress has access to a significant amount of classified material. Classification guidelines, currently based on presidential directives, can be modified by Congress at any time. Extending this principle, Congress, acting as a body, has the authority to declassify and release any information to the public and can remove the secrecy from any information requested by Congress. Fears that Congress cannot be trusted with sensitive information because of the potential for leaks owing to partisan political pressure, although possibly valid, imply that executive agencies do not misuse sensitive information.

Executive privilege, even though only peripherally related to national security, is important, because the rationale that justifies it provides the broadest scope for government secrecy. The policy issues involve a real need for some privately held executive information and an inherent conflict of interest if the president determines which executive department actions are investigated. The prevailing trend, given the traditional deference between those branches, is that, except in extremely political cases where an impeachment inquiry may be possible, the president can safely keep almost any executive department information secret from both the public and Congress.

8.3 Prior Restraint

The First Amendment of the Constitution guarantees that the government will pass no laws that interfere with either free speech or a free press.[24] Neither of these rights is absolute but can be restricted by other government requirements, such as national security. Restrictions are usually applied as legal or monetary sanctions after the violation has occurred. For example, people who disclose classified information can be prosecuted under the Espionage Act, but, unfortunately, the national security damage has already occurred and cannot be undone by punishing the perpetrator. From the perspective of national security, stopping the damage from occurring by preventing the original release of the information would be preferable. Critics of prior restraint argue that it prevents damaging speech by unnecessarily depriving people of their right to protected speech and that disclosure of truly sensitive information can be adequately prevented by penalizing improper speech. Their position can be summarized as "A criminal statute chills, prior restraint freezes."[25] **Table 8-1** identifies some major civil liberties cases.

Table 8-1

Restrictions on Information Flow

Restrictions	Examples of Restraint
Media	
Prior restraint	Pentagon papers
Restricted media coverage	Grenada
Individual	
Secrecy agreements	U.S. v. Snepp
Prior restraint (science)	Export control
Prosecuted for leaking government information	Daniel Ellsberg
Prosecuted for receiving government information	Thomas McAusland, Christopher Pafort

Prior restraint is an ambiguous concept that incorporates many different forms of restraints and can be applied to both individuals and the media. Although the most famous prior restraint cases, the Pentagon papers[26] and *The Progressive*,[27] involved attempts by the

government to prevent publication of "classified" material by the media, other forms of restraint have included: efforts by the government to limit access to national security events, such as military actions; secrecy agreements for government employees that require prior approval of their writing; and controls on scientific communication.

8.3.1 Prior Restraint on Media

The landmark cases in prior restraint of information deal with prior restraint of the media and government employees. The Supreme Court found that because "any system of prior restraints of expressions comes to this Court bearing a heavy presumption against its constitutional validity,"[28] the government can only restrict the publication of material by the media that would cause "direct, immediate, and irreparable damage" to the U.S.[29] Because federal employees have contractual obligations, the government can restrict employees from publishing material "harmful" to the national security,[30] a much lower standard. Because of the different standards, there has been only one case in which the Court allowed prior restraint against the media but several successful prior restraint prosecutions against government employees.

On June 13, 1971, *The New York Times* started to publish the Pentagon papers, a Top Secret history of U.S. involvement in the Vietnam War. The papers were given to the *Times* by Daniel Ellsberg, a former Defense Department employee who had helped write them.[31] The government, fearing damaging political and national security revelations, sued in federal court to prevent further publication. The Supreme Court, although it recognized that prior restraint was constitutional[32] and that the Pentagon papers were officially classified, disallowed the injunction, ruling that the government had not met the heavy burden of proof necessary for prior restraint.[33] The decision showed that classification does not, by itself, justify prior restraint.[34]

One case demonstrates that the burden of proof established in the Pentagon papers case could be met. In 1979, the *Progressive* magazine wanted to publish an article entitled, "The H-Bomb Secret: How We Got It, Why We're Telling It."[35] The article contained information from source material available in the public library. The magazine sent the article to the Department of Energy for classification review. After the magazine refused to modify the article to eliminate material the DOE said was classified, the government, using the Atomic

Energy Act, filed suit to prevent publication.[36] The District Court concluded that the publication threatened "grave, direct, immediate, and irreparable harm to the United States," as specified in the Pentagon papers case, and granted an injunction preventing publication.[37] The effect of the decision was minimal, because the government dropped the prohibition on the basis of the subsequent publication of similar information.[38]

8.3.2 Secrecy Agreements

A more efficient way to protect information is to ensure that the sources of information, especially government employees, do not provide it to the media. Looser standards against prior restraint of publication apply to government employees. Before gaining access to classified material, they must sign a secrecy agreement that requires them to submit all written material on "subjects of interest" to the government for review prior to publication. The government has the right to remove any material that would be "harmful to the national security."[39] The requirement for prior review remains in effect for the lifetime of the employee.[40] CIA regulations, for example, specify that:

> in reviewing manuscripts of former employees, [the CIA board] shall identify and deny permission for publication that information or intelligence which (a) is properly classified, or which reveals intelligence sources or methods, (b) that was acquired by the former employee during the course of his employment, and (c) which has not been placed in the public domain by the U.S. Government.[41]

The constitutionality of secrecy agreements was upheld by the Supreme Court in 1980[42] in the Frank Snepp case.

Snepp, a former CIA analyst, had signed the secrecy agreement while employed by the CIA. After leaving the agency, without gaining prior approval he wrote *Decent Interval*,[43] a book highly critical of CIA involvement in the fall of Saigon.[44] The agency sued on the grounds that the secrecy order was violated. Although the government never claimed that any material in the book was classified[45] and the CIA acknowledged that it had not sued authors of more complimentary books who had not complied with the same secrecy agreement,[46] the Supreme Court ruled that the CIA procedure was necessary to ensure suppression of "harmful" information.[47]

Two other cases involving former CIA employees are relevant to discussion of prior restraint. United States v. Marchetti found that the First Amendment protects the right of government employees to publish unclassified information[48] but that the court had little freedom in examining classification decisions of the executive branch. McGehee v. Casey[49] attempted to challenge the classification process used in the review process directly. McGehee complied with the secrecy agreement after writing an article and submitting it to the CIA for review. After making the requested deletions, he sued, claiming that some of those he was forced to make were from improperly classified material.[50] The court, claiming that the case did not "constitute a prior restraint in the traditional sense upon McGehee," upheld the right of the CIA to determine classification[51], free from judicial review.

The policy questions raised in these cases are concerned with the limits on suppression of information and the impact on the public's interest in understanding the government. By refusing to look at classification decisions, the courts have granted the executive agencies wide discretion for applying prior restraint, especially on government employees. Critics fear that the government could use its power to suppress dissent instead of protecting national security secrets. The wording of the Snepp decision—that prior restraint is acceptable for "harmful" information—leaves the scope of the government's powers ambiguous. The term "harmful" appears similar to the classification definition, "reasonably expected to cause damage to the United States." Whether the government can restrain unclassified information is unclear. Prior restraint decisions have been interpreted both to as approving "suppression of 'harmful' but unclassified information"[52] and as approving limiting the government's authority to only classified information.[53] Snepp's book, by the government's admission, did not contain classified information, yet it was suppressed anyway.

The proper balance between the government's need for secrecy and the public's right to know, although acknowledged by the courts, was never directly addressed by them.[54] Thomas Emerson, Lines Professor of Law at Yale and a critic of excessive secrecy, proposed the following balancing test for questions of prior restraint:

> 1. Constitutional principles protecting freedom of expression occupy a preferred position in the hierarchy of democratic values; hence, there is a presumption in favor of the constitutional right.

2. Government claims of injury to national security must be viewed with a healthy skepticism.

3. The burden of proof to demonstrate its case for limitation rests on the government.

4. The government must show a direct, immediate, grave, and specific harm to national security, not just a vague or speculative threat.

5. The restriction sought by the government must be confined to the narrowest possible constraint necessary to achieve the goal, and should not be permitted where methods having a less drastic effect upon First Amendment rights are available.

6. Whenever possible, hard and fast rules, rather than loose balancing tests, should be formulated and applied.[55]

Prior restraint on publication remains an ambiguous legal concept application of which depends on the changing public attitude toward national security and the dangers of secret government.

8.3.3 Limited Media Access

Prior restraint on the media normally provokes legal battles and public controversy. Another method of accomplishing the same goal is to restrict media coverage of national security events, because what the media does not know cannot be reported. Beyond national security, restrictions on the media are common. Open meeting laws are a familiar approach to the problem of the government operating secretly.

During every military conflict from the War of 1812 through the Vietnam War, reporters had free access to the fighting but were censored by the government. In the war in Vietnam, although censorship was not officially applied in part because technology made that difficult, the news media accepted guidelines for informal security.[56] Censorship of individual stories was unattainable, because the military did not control the movement of civilians in Vietnam. Reporters could go anywhere, even leave the country, to avoid censorship.[57] With the advanced communications technology now available, such as small satellite dishes, the media can easily bypass controlled military channels. A good example of the effect of modern technology on reporting was the coverage of the Marine landing in Somalia in 1992. Having been told by authorities the location and time of the landing, the media broadcast the landing

live,[58] causing the military to complain that the presence of reporters interfered with the military mission. The military took a different approach in the invasion of Grenada in 1983, when it prevented access by the media to the battlefield until after the invasion was completed. Predictably, this action evoked outrage from the media, which claimed violations of the First Amendment violations.[59]

In response to the controversy, the Pentagon developed a media pool to report future military actions.[60] Its members are accredited by the government and would be allowed access, under government control, to war zones at the earliest possible time. To enhance security, the members of the pool would be called at the last moment and assembled secretly. Their security guidelines would be similar to those used during the war in Vietnam.[61] The pool was used in 1989 in the invasion of Panama and in 1990–91 in operation Desert Storm.

The reporters in Desert Storm had access to combat areas, but only with military escort. They were limited to trips arranged by the military and often restricted from actual combat, as in the case of the Khafji fighting. Their stories were subjected to a security review.[62] In response to these restrictions, some media organizations sued, saying that the restrictions constituted unconstitutional prior restraint. The war ended before the case was heard, and the court dismissed the action without ruling on the constitutional questions.[63] Although the standard for prior restraint is high, access restrictions have lower standards. The courts have said that "the door to freedom of access is narrower and only leads to where the general public may freely go."[64] In order to deny access, the government has only to show that the restrictions serve a government interest and that their primary purpose is not to prevent the media from acquiring information.[65]

The media believes its First Amendment rights are being violated. To cover the news, in particular military actions, accurately, it needs unrestricted access and uncensored reporting, within the bounds of accepted security agreements.[66] The media feels its responsibility to ensure that the public has access to complete and accurate information requires it to go beyond the limits imposed by the military. The military, concerned with protecting sensitive information about operations and plans as well as with providing for the safety of both soldiers and reporters, feels it must limit access by the media. In prior wars, access by the media was not a critical issue, because the time delay between reporting and publishing news

made censorship practical. New technology that allow live broadcast of the war on international television eliminate the safety of a time delay. Without controls on the media, instantaneous and unedited information about U.S. forces might be available to adversaries,[67] potentially at a great cost in lives and resources. Studies such as the Sidle panel (the Chairman, Joint Chiefs of Staff [CJCS] Media-Military Relations Panel), which recommended the pool structure,[68] concluded that the press pool is the best possible compromise between the needs of the press and the overriding needs of national security.

Unanswered in the argument over media access is the validity of considering national morale as an integral part of national security. The information reported by the media, although not classified, shapes public debate. The media argues that the primary reason the government limits access to the battlefield is to manipulate public debate, not to protect sensitive information. Questions about the proper role of public opinion in national security, the right of the government to censor nonsensitive information in the name of national security, and the responsibility of the press to self-censor its reporting in order to avoid skewing the debate must be addressed in balancing the rights of the government and the press.

The question of how public opinion should be factored into the national security cannot be resolved factually. Press coverage of the war in Vietnam provided ample evidence that "negative" battlefield reportage, although not militarily sensitive, influences the public debate. Many people felt that the war was lost on television through the unrelenting stream of negative stories about the war. They felt that television images caused the public to believe that the war could not be won and was not worth fighting. It might be argued that by helping to turn the American public against the war, the media hampered the war effort and hurt national security. If true, people could argue that national security requires some media restrictions once the government has embarked on military action. Even if the premise that adverse public opinion damages national security is accepted, drawing a boundary between acceptable security restrictions and government manipulation of the news is probably impossible, because informed public debate remains necessary during war. Alternatively, it can be argued that any limitation on the media that prevent an informed public debate lead to an even greater problem by removing the national consensus necessary to conduct a war successfully.

8.3.4 Theft of Information

In 1992 a new form of prior restraint was provided[69] when an appeals court agreed that unauthorized receipt of unclassified government information represents theft of government property. The 4th Circuit Court of Appeals upheld a one-year jail sentence against Thomas McAusland and Christopher Pafort, employees of Litton Data Systems,[70] who were accused of receiving unclassified but unreleased information about Litton contract proposals from a consultant. They were convicted under 18 USC §641, which imposes criminal sanctions on anyone who "embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money or thing of value of the United States." The court found that "the defendants could be convicted of conversion of government property. . .and it was not necessary that disclosure be clearly prohibited by published federal acquisition regulations."[71] Although this ruling is precedent only for the 4th Circuit, in late 1992 the Supreme Court refused to hear an appeal.[72] The possibility that the principle in this ruling could be used against reporters investigating government corruption through government leaks, although not discussed in the opinion, is clear. Given the preliminary nature of the issues, the actual implications of the opinion for government openness remain unknown.

8.3.5 Scientific Communication

Another form of prior restraint is concerned with restrictions on scientific communication. Secrecy clashes with the open communication crucial to scientific advances. The development of new and better technology is at the heart of improving U.S. economic competitiveness. Stifling scientific advances, even for national security, has obvious negative economic consequences.

Mechanisms for restraint on scientific communication, such as classification and export control, need to be understood in the context of prior restraints. Publication of scientific communications, like other forms of publication, can cause damage that no postpublication penalties can undo. All the scientific restrictions are therefore aimed at preventing possibly damaging communication, not at punishing an inappropriate communication. The policy issues of restricting scientific communication are similar to those in other forms of prior restraint.

The greatest negative effect of prior restraint on civil liberties is that of inadvertent prohibition on protected communication. The rules that regulate the restrictions must necessarily be broad in order to inhibit all damaging information, in whatever form. Interpretations of the regulations will vary. Consequently, people fearful of accidentally violating regulations tend to shy away from publishing anything remotely close to the areas restricted. The publication of a lot of information that could be released will therefore be prevented. In some cases, this prevention of publication is a minor matter, but not for scientific communication. Unfortunately, determining a priori what results or theories might be important to science in the future is almost impossible. Prior restraint will both restrict information necessary to technological advancement in the U.S. but at the same time not restrict results that may help other countries develop technology harmful to the U.S. Determining the precise boundaries for prior restraint on scientific communication entails figuring out how not to do more harm than good.

8.4 Privacy

The flip side of secrecy is the invasion of privacy,[73] either by government or through activities sponsored by it. Although the scope of privacy rights was never explicitly formulated in the Constitution, most Americans believe they have a fundamental right of privacy that should not be lost because of government action. Even though individual privacy does not directly concern national security, many of the issues involved in assuring privacy impact on the government's secrecy policy.

Privacy introduces another restraint on government openness. Recognizing that individual privacy was important to the public, Congress provided an exception to the FOIA in the Privacy Act. These laws attempt to balance the right of access to government information with the expectation of privacy. The FOIA exempts from public release "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[74] Before the release of personal information, the government has to "weigh the severity of the invasion against the public's interest in disclosure."[75] The Privacy Act protects against the misuse of personnel information collected by the government. It requires federal agencies to "permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose."[76]

8.4.1 The Privacy Act

Privacy rights and national security requirements present similar problems, especially in deciding scope and limitations and in balancing competing rights. The FOIA was adopted because the government tended to prohibit the release of information, even information that should be released. Refusing to list all possible types of personal information in the government's hands, Congress wrote the ambiguous privacy exception into the FOIA that defines personnel, medical and "similar files" eligible for protection. The danger, like that of overclassification, is that a broad interpretation could inappropriately justify keeping information secret.

Early case law[77] developed the idea that "similar files" needed to contain "intimate details" of a "highly personal nature" in order to qualify—highly subjective concepts that require case-by-case decisions. The Supreme Court expanded the concept of "similar files" to include "detailed Government records on an individual which can be identified as applying to that individual."[78] Any government information, therefore, that identifies a private individual can be denied if the government determines that the right of privacy outweighs the benefit of public disclosure.

Opponents, especially the media, attack the court decision on the grounds that it encourages excessive government secrecy. Reminiscent of the classification debate, the government is given wide discretion in determining the balance between fundamental rights. Critics claim that such discretion will allow the government to "wave privacy around any time the public or press make requests for information which might prove embarrassing to government officials."[79] Similarities to classification include: no clear-cut criteria for determining what constitutes privacy; possible abuse of the process by people with ulterior motives; a tendency toward prohibiting release because it might cause immediate damage; and diffuse organizational responsibilities, which make consistent decisions across the government impossible.

8.4.2 Privacy Technology

Strong privacy technology, such as commercial cryptography, presents the government two problems. Commercialization of the technology could damage national security (see **Chapter Six**). Strong mechanisms could prevent authorized access to personal information of

U.S. citizens for the purpose of law enforcement and other legitimate government activities. The 1990s version of the debate represents the latest saga of a continuing battle. Similar civil rights issues were raised in the 1700s over the privacy of mail in the government-controlled postal system and in the 1800s over the privacy of commercial telegrams.[80] The application of protection technology has to make the delicate balance between individual privacy, the economic benefit gained by protection of commercial information, the national security ramifications of allowing the commercial use of sensitive technology, and the ability of the government to conduct its activities.

The government uses many methods to protect national security information, including technologies such as encryption and computer security, which are equally useful for protecting individual privacy. For brevity, this section examines only cryptography, although the tradeoffs discussed here hold for other technologies.[81] Cryptography (see **Chapter Six**) can be used to protect government, business, and personal information. One mechanism used by intelligence agencies is interception by electromagnetic signals. The primary reason given by the government for export controls on commercial cryptography is to prevent an adversary from using superior U.S. technology to hamper attempts by the U.S. intelligence community to gain this information. Similarly, within the U.S., during investigations of suspected criminal activities the law enforcement community can obtain court orders for wiretaps. Although the mechanism for intercepting information is not the same in both cases, encryption technology impedes both activities.

8.4.3 Law Enforcement Requirements

In 1991 and 1992 the FBI proposed legislation[82] in an effort to safeguard access of the law enforcement community to wiretap information, which it perceived in increasing danger of obsolescence because of increasingly sophisticated communication technology.[83] The FBI proposed a "Sense of Congress" resolution in the 1991 Omnibus Crime Bill that would have required communication and computer firms to supply a plain-text version of any information processed by their equipment.[84] The resolution failed. In 1992, the FBI returned with a proposal to equip all digital communication equipment with a remote monitoring capability which the FBI could use to conduct wiretaps.[85] The proposal was withdrawn after extensive controversy.

On April 17, 1993, President Clinton introduced a new government cryptographic technology, the Clipper Chip—designed to cost $25—which includes a key management system that would allow the government to decrypt information encrypted by the chip. The president proposed the establishment of a central clearinghouse for the decryption information. When a court order for a wiretap would be obtained, the clearinghouse would provide the government with the decryption material.[86]

The FBI believes that it must find a way to tap digital technology or advancing technology will make legitimate law enforcement wiretaps obsolete. Digital communication equipment, which is rapidly replacing analog equipment, changes the way information is processed and transmitted. Analog technology was mainly circuit-switched, so that each call is transmitted on an individual circuit that could easily be isolated and intercepted, but digital systems bundle many lines together which cannot easily be isolated. Wiretaps are, of course, a relatively recent phenomenon, which originated with the introduction of the telegraph, telephone, and radio. As recently as the 1930s, legal and ethical debate on wiretaps was widespread.[87] The Federal Communications Act of 1934 forbids interception and divulging of "interstate or foreign communication by wire or radio."[88]

The wiretap proposals introduce serious economic and privacy policy issues. Advocates claim the proposals do not raise any new policy issues but merely clarify current laws and law enforcement practices. According to the former director of the FBI, William F. Sessions, the 1968 Omnibus Crime Control and Safe Streets Act

> requires telephone companies to assist law enforcement in implementing wiretaps. What has been proposed is legislation that clarifies the duties of the telephone service providers in responding to court orders. . .in other words, [they] continue to maintain their current ability.[89]

Opponents believe implementation of the proposals raises new civil liberties and technical security issues. They believe the security of the overall communications network might be jeopardized by putting in mechanisms for tapping phones or weakening the cryptography protection. Because the President's proposed Clipper Chip[90] is the latest development, the policy questions it raises—including the security provided by the chip, its effectiveness, the possibility of government abuse, and the propriety of government competition against private companies—provide the focus for the following discussion.

Critics question the strength of the Clipper chip. Its algorithm, like DSS (**Chapter Six**), was developed secretly by NSA, but, unlike DSS, it will remain secret, leaving users no way to evaluate its cryptographic strength. The decryption keys will be held by "two independent entities," unknown in August 1993,[91] raising questions about the security of the keys. The keys would be a tempting target for hackers, national and industrial espionage, criminals, media, politicians, or government agents. Whether today's technology can provide the necessary degree of security is still not clear.

The chip's effectiveness in preserving law enforcement techniques is questioned. Widely available encryption equipment already can defeat any FBI wiretap. Because encryption negates the FBI capabilities, critics worry that the current proposal is the first step toward outlawing all other encryption products. State law enforcement agencies use wiretaps, but, as defined in May 1993, the keys would be available only to the FBI, not to local and state law enforcement agencies. If true, this preserves the ability of federal law enforcement at the expense of state agencies. If the keys were provided to state agencies, their increased exposure might increase the danger of compromise.

A major criticism is the potential for government abuse. According to Stephen Byren, a former Pentagon official, "People won't be able to trust these devices because there is a high risk that the Government is going to have complete access to anything they are going to do."[92] Supporting this fear is the fact that the decryption key remains constant, allowing the FBI to continue to tap the chip after the court order expires. This threat is not new: the FBI can abuse the present system by tapping telephones without a court order.

A central policy question in civil liberties is the degree to which the government should go to accomplish its objectives. The Crime Bill of 1968 gives the FBI authority to conduct wiretaps, but the Clipper chip goes further. It sets up the government as a direct competitor to commercial cryptography vendors,[93] because the government sponsors the manufacture of the chip. The government will encourage consumers to buy its product, at the direct expense of existing manufacturers of commercial cryptography.

These proposals potentially hurt both national security and economic competitiveness. In an age of increased competitiveness,[94] many businesses rely on encryption to protect

economically valuable information. Reducing the protection afforded corporate information increases the possibilities of losing that information to foreign competitors, through industrial or national espionage. Technology transfer hurts both the economy and national security (**Chapter Seven**). Another effect might be potential loss of international sales of digital communications equipment, in 1991 $2.5 billion.[95] International buyers might not want such equipment if they felt that the U.S. government was able to decrypt their information. The basic tradeoff is the legitimate need of the government to gather selected information within the U.S. as opposed to potential problems in national security, economic competitiveness, and individual privacy.

Excessive secrecy strikes at the heart of the people's fundamental right to know about the government. Although the government must balance reasons for secrecy based on national security, many techniques examined in this chapter have little to do with national security and more to do with political debate in the U.S. Techniques for achieving civil secrecy, such as executive privilege and privacy regulations, are extremely wide-ranging and ease falling into the trap of manipulating information instead of protecting it. Careful policy consideration needs to be given to what constitutes information that while sensitive does not endanger national security and what constitutes government manipulation of information.

Notes

1. James Madison, cited in John Shattuck, "Explorations: National Security a Decade after Watergate," *democracy* (Winter 1983); reprinted in *1984: Civil Liberties*, 406.

2. Prior to 1952, executive privilege had been claimed fewer than twenty-five times. Between 1952 and 1972, it was claimed at least fifty times. Lewis, *None of Your Business*, 14-15.

3. In his opening statement, Sen. Sam Ervin cited the following numbers: Between 1965 and 1973 there were more than 130 instances of executive departments refusing either to testify or submit documents to Congress, with executive privilege formally invoked in only a few of them. U.S. Congress. Senate. Subcommittee on Intergovernmental Relations of the Committee on Government Operations. Subcommittee on Separation of Powers and Administrative Practice and Procedures of the Committee on the Judiciary. *Executive Privilege Secrecy in Government Freedom of Information*, Vol. 1, 93rd Cong., 1st sess., 5; hereafter, *Executive Privilege*. The specific number of times executive privilege was formally invoked has been disputed. One study by the Library of Congress, made in 1973, showed that Kennedy invoked executive privilege thirteen times, Johnson twice, and Nixon nine times. A second study by the Library of Congress, also in 1973, increased Nixon's total to nineteen. Sen Hugh Scott, R.-Penna., disputed that number, claiming that Nixon had used executive privilege only three times. Jim Eatherton, "Executive Privilege: An Unresolved Legitimacy Problem," *Freedom of Information Center Report No. 501* (School of Journalism, University of Missouri at Columbia, November 1984), 7.

4. Norman Dorsen and John Shattuck, "Executive Privilege, Congress, and the Courts," speech presented by Norman Dorsen at the Ohio State Law Forum, April 23, 1973; reprinted in *Executive Privilege*, Vol. 3, 159.

5. Ibid.

6. Memorandum of Attorney General William Rogers submitted to the Subcommittee on Constitutional Rights of the Committee on the Judiciary, U.S. Senate, 85th Cong., 2nd sess., 1958.

7. Raoul Berger, "Executive Privilege V. Congressional Inquiry," *UCLA Law Review*, Vol. 12: 1043, 1965; reprinted in *Executive Privilege*, Vol.3, 2.

8. Ibid., 36. Claims of executive privilege were first raised in the Washington administration during the Congressional investigation of the St. Clair Expedition. During cabinet discussion about a Congressional investigation, Jefferson records that the cabinet concluded that 'the executive ought to communicate such papers as the public good would permit and out to refuse those the disclose of which would injure the public.' To support his case, Jefferson cited English precedent in the case of the Parliament investigation of S. Rob. Walpole.

9. The history of executive privilege presented here was derived primarily from Raoul Berger, *Executive Privilege*, Vol. 3, 1-140.

10. Parliamentary inquires into executive actions are documented for 1604, 1621, and 1666.

11. Berger, *Executive Privilege*, Vol. 3, 15.

12. McGrain v. Daugherty, 273 U.S. 135, 174 (1927), quoted in *Executive Privilege*, Vol. 3, 16.

13. 1 Stat 65-66 (1789) 5 U.S.C. 242 (Supp. V, 1959-1963), quoted in Berger, *Executive Privilege*, Vol. 3, 14.

14. The provision was written by Alexander Hamilton with the idea that he, as the first Secretary of the Treasury, would be able to have a conduit to Congress in order to express his views on monetary issues. The Congressional debate centered on the fear that too much information would be sent to Congress.

15. Berger, *Executive Privilege*, Vol. 3, 19-20, cites Attorney General Rogers in a 1958 memorandum: "One of the most powerful arguments to be found anywhere for the right of the President and the heads of the departments to withhold confidential papers. . .in their discretion. . .is contained in the history dealing with the creation of the Department of Foreign Affairs by the Continental Congress in 1782. . . . The members who sat in the New Congress in 1789 could not have been unfamiliar with the fact that during the existence of the Continental Congress its Members had been entitled to see all kinds of secret data. The conclusion is therefore inescapable that the founders of our Government, and those who sat in the First Congress, meant to give no power to the Congress to see secret data in the executive departments against the wished of the President. This was a power which the Continental Congress had and which the framers of the Constitution meant for the new Congress, created by the Constitution, not to have."

Proponents cite Attorney General Cushing's advice in 1854: "By express provision of law, it is made the duty of the Secretary of the Treasury to communicate information to either House of Congress when desired; and it is practically and by legal implications the same with the other secretaries." Berger, *Executive Privilege*, Vol. 3, 21.

16. 45 Stat 986-96 (1928), 5 USC §105a (1958).

17. Berger, *Executive Privilege*, Vol. 3, 50.

18. President Jefferson, responding to a request for information in U.S. v. Burr, 25 Fed Case (No. 14693) said: "Reserving the necessary right of the president of the United States to decide, independently of all other authority, what papers coming to him as president the public interest permits to be communicated, and to who, I assure you of my readiness, under that restriction, voluntarily to furnish on all occasions whatever the purposes of justice may require." Cited by Attorney General Kleindienst, letter to Senate (May 15, 1973), in *Executive Privilege*, Vol. 3, 212.

19. Dorsen and Shattuck, "Executive Privilege, the Congress, and the Courts," 160.

20. Kleindienst, *Executive Privilege*, Vol. 1, 25.

21. United States v. Nixon, 418 U.S. 683, 1974.

22. Todd D. Peterson, "Criminal Contempt of Congress," *New York University Law Review*, Vol 66:563, 615.

23. Peterson, "Criminal Contempt of Congress," 573. On December 11, 1982, the House issued a Contempt of Congress citation to Anne Boursch, Administrator of the Environmental Protection Agency, for refusing to deliver documents to Congress. The president tried to get the citation revoked in Federal Court, but the court refused to hear the case, recommending further negotiations. The citation was eventually revoked after a successful agreement between Congress and the President allowed the documents to be reviewed. Jim Eatherton, "Executive Privilege: An Unresolved Legitimacy Problem," P.1. Congress also brought contempt charges

against Secretary of the Interior James Watts, but the matter was dropped after he turned the documents to Congress.

24. United States Constitution, First Amendment.

25. A. Bickel, *The Morality of Consent* (1975), cited in Stanley Godofsky and Howard M. Rogatnick, "Prior Restraints: The Pentagon Papers Case Revisited," *Cumberland Law Review*, Spring 1988, **18**, 540.

26. New York Times v. United States, 403 U.S. 43 (1971).

27. United States v. Progressive, Inc., 467 F. Supp. 990 (W.D. Wis.).

28. New York Times v. United States, 403 U.S. at 714, cited in Godofsky and Rogatnick, "Prior Restraints: The Pentagon Papers Case Revisited," 529.

29. Ibid., 541.

30. Snepp v. United States, 444 U.S. 511-512, discussed in Diane F. Orentlicher, "Snepp v. United States: The CIA Secrecy Agreement and the First Amendment," *Columbia Law Review*, April 1981, 685-686.

31. Halperin and Hoffman, *Top Secret*, 5-14.

32. Near v. Minnesota, 283, U.S. at 716 (1931) first established that the concept of prior restraint for national security purposes in some circumstances was constitutional. According to the decision, "a government might prevent. . .the publication of the sailing dates of transports or the number and location of troops."

33. New York Times v. United States, 403 U.S. at 714.

34. Godofsky and Rogatnick, "Prior Restraint: The Pentagon Papers Case Revisited," 530.

35. Ibid., 541.

36. Wreden, "Prior Restraint and the Progressive," P.1-P.2.

37. Godofsky and Rogatnick, "Prior Restraint: The Pentagon Papers Case Revisited," 541.

38. *The Milwaukee Journal* published a similar piece on April 30 and May 1, 1979. Also, a student found declassified DOE documents at the library of the Los Alamos Laboratory that revealed far more detailed information than the article in *The Progressive*. Nick Wreden, "Prior Restraint and the Progressive," P.3.

39. Snepp v. United States, 444 U.S. 511-512.

40. Ibid. The Supreme Court placed an injunction on Snepp requiring review by the CIA prior to publication of all his future writings related to intelligence.

41. Central Intelligence Agency Publication H.R. 10-7, "Non-Official Publication by Employees and Former Employees," dated 1 March 1977, cited in U.S. Congress. House. Subcommittee on Oversight of the Permanent Select Committee on Intelligence, *Prepublication Review and Secrecy Agreement*, 96th cong., 2nd sess., 1980, 9. Although this agreement was superseded in August 1983 by President Reagan, the new agreement is similar. Required of anyone with access to Special Compartmented Information, the new one extends beyond the intelligence community to bring thousands of additional employees under secrecy

agreements. Floyd Abrams, "The New Effort to Control Information," *New York Times Magazine*, September 25, 1983, cited in *1984: Civil Liberties*, 396-397.

42. Snepp v. United States, 444 U.S. 507 (1980) (per curiam).

43. (N.Y.: Random House, 1977).

44. The discussion of the Snepp case was generated by Orentlicher, "Snepp v. United States: The CIA Secrecy Agreement and the First Amendment," 662-706.

45. 595 F.2d at 935.

46. Orentlicher, "Snepp v. United States: The CIA Secrecy Agreement and the First Amendment," note 9, 664.

47. 444 U.S. at 511-12.

48. Marchetti v. United States, 466 F.2d 1309 (4th Cir). The argument about unclassified information was developed by Orentlicher in "Snepp v. United States: The CIA Secrecy Agreement and the First Amendment," 685-686.

49. McGehee v. Casey, 718 F.2d 1137 (D.C. Cir. 1983).

50. Godofsky and Rogatnick, "Prior Restraint: The Pentagon Papers Case Revisited," 544.

51. Ibid., 544-546.

52. Justice Stevens in his dissenting opinion (ibid., at 522), cited in Orentlicher, "Snepp v. United States: The CIA Secrecy Agreement and the First Amendment," note 163, 686.

53. Ibid., 686. Justice Stevens also stated that he did "not understand the Court to imply that the Government could obtain an injunction against the publication of unclassified information." Agee v. CIA, 500 F. Supp 506,508 (D.D.C. 1980) has interpreted prior restraint to apply only to classified information.

54. Orentlicher, "Snepp v. United States: The CIA Secrecy Agreement and the First Amendment," 706.

55. Thomas I. Emerson, speech at Institute for Communications Law Studies of Catholic University School of Law, December 1983, printed in *Communications Lawyer*, Winter 1984, reprinted in *1984: Civil Liberties*, 422.

56. Gottschalk, "American Military Press Censorship," 463.

57. Ibid., 477.

58. Johanna Neuman, "Military's Photo Op 'Got Out of Hand,'" *USA Today*, Dec. 10, 1992, 1. Although the military had given the media the location and time of the landing and given them permission to cover the landing, the resultant coverage took the military by surprise.

59. For a sampling of stories about the controversy surrounding exclusion of the media in Grenada, see *1984: Civil Liberties*, 481-505.

60. This structure of the pool was based on the CJCS Media-Military Relations Panel (Sidle Panel) set up after the Grenada invasion to examine the question of media coverage. A copy of the report is printed in *1984: Civil Liberties*, 432-446.

61. Richard Halloran, "Pentagon Forms War Press Pool; Newspaper Reporters Excluded," *New York Times*, Oct. 10 1984; reprinted in *1984: Civil Liberties*, 508.

62. Michael W. Klein, "The Censor's Red Flag, the Bombs Bursting in Air: The Constitutionality of the Desert Storm Media Restrictions," *Hastings Constitutional Law Quarterly*, **19**, 4 (Summer 1992), 1050.

63. Nation Magazine v. United States Department of Defense, 762 F. Supp. 1558.

64. In Branzburg v. Hayes, 408 U.S. 665, the Supreme court ruled that the press did not have a constitutional right of special access to information not available to the public generally. Other judicial opinions suggest that the media does have some minimal right and responsibilities to report foreign military operations, among them the court decision on the *Nation*, which said: "There is support for the proposition that the press has at least some minimal right of access to view and report. . .including. . .an overt combat operation' and Justice Black in his Pentagon Papers opinion which said 'among the responsib-ilities of a free press is the duty to prevent any part of the government from deceiving the people and sending them off to distant lands to die of foreign fevers and foreign shot and shell" (Klein, "The Censor's Red Flag, the Bombs Bursting in Air," 1061, 1067).

65. Ibid., 1063.

66. During the war in Vietnam the Defense Department pulled the credentials from only six reporters, for publishing information contrary to the security agreement they signed when accredited. Gottschalk, "American Military Press Censorship," 477.

67. For example, in Somalia internationally televised pictures of the marine landing showed militarily useful information such as where the troops were landing, how many troops were involved, their equipment, and their formation. In other circumstances, such information could have been used in attacking the troops.

68. CJCS Media-Military Relations Panel (Sidle Panel). A copy of the report is printed in *1984: Civil Liberties*, 432-446.

69. 979 F.2d 970 (4th Cir.[Va.]) 1992.

70. "Men Jailed Because They Knew Too Much," *Information Industry Bulletin*, **9**, 13, April 8, 1993, 1-4.

71. 979 F.2d 970 (4th Cir.[Va.]) 1992.

72. "Men Jailed Because They Knew Too Much," 3.

73. For a useful historical introduction to this issue, see David J. Seipp, *The Right to Privacy in American History* (Cambridge, Mass.: Harvard University Program on Information Resources Policy, P-78-3, July 1978).

74. 5 USC §552 (b)(6).

75. Jeanne Abbott, "Exemption 6: Privacy under the Freedom of Information Act," *Freedom of Information Center Report No. 476*, School of Journalism, University of Missouri at Columbia, June 1983, P.2.

76. Privacy Act, PL 93-579, §2(b)(2).

77. Getmen v. National Labor Relations Board, 450 F.2d 670 (D.C. Cir 1971) provided the initial legal reasoning. Abbott, "Exemption 6: Privacy under the Freedom of Information Act," P.2.

78. U.S. Department of State v. Washington Post Co., 456 U.S. 595, 102 S. Ct. 1957 (1982).

79. Jack Landau, Director of the Reporters Committee for Freedom of the Press cited in Abbott, "Exemption 6: Privacy under the Freedom of Information Act," P.5.

80. Seipp, *The Right to Privacy in American History*, 7-16, 30-42.

81. Anecdotal evidence suggests that the government asked some manufacturers of computer software to place a "back door" in software so the government can, if necessary, bypass the security mechanisms to gain access to information. RISKS-Forum Digest, Peter G. Newman, moderator, Forum on Risks to the Public in Computers and Related Systems, ACM Committee on Computers and Public Policy, 14.33, Feb. 6, 1993. [electronic bulletin board]

82. A good introduction to the issues involved in the FBI wiretapping proposals can be found in Dorothy Denning et al., "To Tap or Not to Tap," *Communications of the ACM*, **36**, 3 (March 1993), 25-44.

83. Mitch Betts, "FBI Seeks Right to Tap All Net Services," *Computerworld*, **26**, 24 (June 8, 1992), 1.

84. Senate Bill 266 introduced the 1991 proposal. Barlow, "Decrypting the Puzzle Palace," *Communications of the ACM*, **35**, 7 (July 1992), 26.

85. Betts "FBI Seeks Right to Tap All Net Services," 10. The main provisions of the 1992 proposal include:

- Providers of electronic communications services and private branch exchange operators shall provide with the U.S. [the] capability for the government to intercept wire and electronic communications when authorized by law.
- Intercepts must be made in real time, undetectable by the suspect and routed to a remote government monitoring site (Brock N. Meeks, "FBI Wants Digital Snoop Power," *Whole Earth Review* (Fall 1992), **76**, 72).

In July 1992 a second version of the bill eliminated two controversial proposals. The first version also would have the FCC establish and enforce the technical standards and allow telephone companies to charge ratepayers for modifications to their equipment. The second version made the Justice Department responsible for enforcement, while prohibiting the charges to ratepayers.

86. Statement by the White House Press Secretary, "Questions and Answers about the Clinton Administration's Telecommunications Initiative," April 16, 1993.

87. Seipp, "The Right to Privacy in American History," 108-111. In the 1930s, wiretapping was vigorously debated; in 1931 J. Edgar Hoover said: "We have a very definite rule in the bureau that any employee engaging in wiretapping will be dismissed from the service of the bureau. . . . While it may not be illegal, I think it is unethical, and is not permitted under the regulations by the Attorney General. In 1928 in Olmstead v. United States, the Supreme Court upheld wiretapping by a five to four majority. In 1937 and 1939, the Court threw out two convictions based on evidence from wiretapping.

88. 1934 Federal Communication Act, 48 Stat. 1103, June 19, 1934.

89. William S. Sessions, "Wiretap Proposal Isn't Radical," *Computerworld*, **26**, 22 (May 25, 1992), 10.

90. A good discussion on the Clipper chip proposal can be found in RISKS-Forum Digest, **14**, issues 52-55 [electronic bulletin board].

91. Statement by the White House Press Secretary, "Questions and Answers about the Clinton Administration's Telecommunications Initiative," April 16, 1993.

92. Quoted in Markoff, "New Communication System Stirs Talk of Privacy vs. Eavesdropping," 1.

93. Statement by the White House Press Secretary, "Questions and Answers about the Clinton Administration's Telecommunications Initiative," April 16, 1993, 1.

94. Robert Green, "Foreign Espionage Seen as Threat to U.S. Economy," *Reuters Business Report*, April 29, 1992. Sessions and Robert Gates, Director of the CIA, told Congress spying by foreign intelligence agencies against U.S. companies was growing. Sessions mentioned that the former director of the French intelligence service had admitted in an interview that the French spied on U.S. companies and businessmen (although the actual number of instances was quite small). [NEXIS]

95. U.S. Department of Commerce, International Trade Administration, *U.S. Industrial Outlook 92* (Washington, D.C.: Government Printing Office, 1992), 29-1.

Chapter Nine

Policy Themes

> Interest groups must advocate. . . . They must acknowledge that even with an acceptable utilitarian calculus, the choice involves competing wrongs.
>
> Gary T. Marx[1]

9.1 Themes

The discussion of individual policies in the preceding chapters implies that secrecy was more than a series of unrelated, independent policies that regulate separate missions. Actually, secrecy policies are inextricably linked and rely on a combination of mechanisms to achieve their overall objectives. Because these policies are closely correlated, many important issues and themes recur in a number of them. Although in each secrecy policy some unique issues surface, the decisionmaker is continually faced with certain fundamental tradeoffs involving security, economics, and civil liberties. For example, increasing the priority of economic competitiveness requires fewer export controls, fewer restrictions on technology development, and more open investment. Understanding the relationships among the tradeoffs clarifies the effects of decisions and promotes consistent decisions. This chapter examines themes common to multiple secrecy components and the meaning of the tradeoffs for overall secrecy policy.

9.1.1 Common Tensions

The same unresolvable tensions constantly recur in individual secrecy components, because they do not lend themselves to obvious compromises. Advocates often attempt to manipulate the argument by framing the problems as all-or-nothing propositions; to achieve one objective requires sacrificing all others.[2] Unfortunately, the problems persist, because usually no universally satisfactory or everlasting solutions are available, despite the best efforts of many people. Common tensions arise in:

- picking the proper secrecy objectives
- setting the proper scope of the secrecy controls
- balancing national security benefits against economic costs
- balancing national security against social costs

- balancing national security against social costs
- conforming to political realities

Table 9-1 summarizes the effects of these tensions on specific policies discussed here.

9.1.2 Conflicting Missions

Each secrecy policy represents a compromise between separate, often competing and conflicting, missions. National security objectives are not one-dimensional but acknowledge the necessity for both military and economic strength.[3] No one policy embodies a perfect solution to any specific mission but only a compromise that best meets the needs of different missions. For example, the technology transfer policy has the conflicting missions of permitting economically beneficial transfers while protecting national security technology. The tradeoffs include limiting the objectives of the policy to meet a subset of requirements or providing less than the optimal solution for all requirements of the relevant missions.

One observable consequence of conflicting missions is complex policies. The five-hundred pages of export control regulations illustrate the complexity. The regulations could be simplified, but to do so would hurt one objective, at least in the eyes of those responsible for the missions: a shorter, loosely defined list would result in confusion about which technology was controlled, which would hurt economic competitiveness, while just deleting a technology from the list would damage national security. In the post-Cold War environment, the likelihood is that, without a unifying factor such as the former Soviet Union once supplied, national security objectives will become even more diverse, resulting in continuation of complex compromises among missions.

9.1.3 Ambiguous Scope

To define clear, precise boundaries between proper national security concerns and private concerns is almost impossible. These nebulous boundaries foster inadvertent abuse, because they offer those who implement policy little guidance on the limits of secrecy. Classification, "the unauthorized disclosure of [information] which could reasonably be expected to cause damage," illustrates the problem. The traditionally expansive definitions of national security adequately encompass most national security information, but at the cost of unnecessarily affecting large quantities of non-national security information. More precise definitions of national security would reduce but not eliminate inappropriate controls on information and

Table 9-1

Summary of Secrecy Policies

	Advantages	Disadvantages
CLASSIFICATION		
➢ **National Security**	Address need of national security community to protect operational information Address need of national security technology for protection from indiscriminate technology transfer	Can keep information from people who need it Can cause waste in defense budget by preventing debate about military expenditures
➢ **Economic Competitiveness**	Protect technology from foreign exploitation	Slow advancement of technology by preventing scientific communication Keep useful defense technology from commercial exploitation High cost
➢ **Civil Liberties**	NA	Impose restrictions on free publication of information guaranteed by the First Amendment Keep information out of the public debate Allow politicians and bureaucrats to hide embarrassing information from the public
EXPORT CONTROLS		
➢ **National Security**	Help maintain U.S. technological lead against adversaries Help prevent proliferation of weapons of mass destruction Can be used to control national security-related technologies Help to lower defense budgets	Discourage the development of some useful national security technologies Can be subverted through espionage, actions of other countries, or reinvention of the technology
➢ **Economic Competitiveness**	NA	High cost to exporters through lost sales, compliance costs, and market-share Provide disincentives to invent new high-technology products Control lists too large, thus controlling dual-use technology vital to U.S. economy U.S. often imposes unilateral controls
➢ **Civil Liberties**	NA	Limit effectiveness of some technologies the public requires, e.g., commercial cryptography

Table 9-1 continued

	Advantages	Disadvantages
TECHNOLOGY TRANSFER CONTROLS		
➤ **National Security**	Investment controls protect U.S. technology from foreign exploitation Help prevent development of security dependency situation Convert useful defense technology to U.S. firms Prop up the U.S. defense industrial base Military sales support U.S. allies	Defense conversion loses control of the technology, allows possible future exploitation Defense technology, e.g., cryptography, used to hurt national security
➤ **Economic Competitiveness**	Provide new technology to U.S. industry FMS provide sales to U.S. defense industry Encourage increased R&D	Prevent full exploitation of technology FDI may prevent necessary sale of defense firm
➤ **Civil Liberties**	Introduce dual-use technology that could be useful, e.g., strong commercial cryptography	Prevent full utilization of technologies introduced
CIVIL LIBERTY CONTROLS		
➤ **National Security**	Protect privacy of personal information contained in government files Provide president with necessary protection for executive information Protect national security information from release	Prevent informed public discussion of U.S. defense policy, which may lead to withdrawal of public acceptance
➤ **Economic Competitiveness**	NA	NA
➤ **Civil Liberties**	Protect privacy	Place controls on public speech Allow government to manipulate public debate Allow president to hide information from Congress and the people by preventing oversight of the executive branch Limit the technology that can be used to protect civil liberties

NA = not applicable

would increase the danger of leaving damaging information unprotected. Given the critical national security mission, the errors of the national security community in defining its scopewill naturally lean toward preventing leaks of damaging material.

The tendency to overprotect information is evident in such diverse activities as classification and technology transfer. The classification system overprotects through overclassification and lack of declassification. Overprotection in export control can be seen in the regulation of dual-use technology, such as computers and telecommunications equipment. Dual-use technology promotes beneficial economic competitiveness, but even when the technology is widely used in numerous other countries, the U.S. government insists on maintaining export controls.

Most people agree that some secrecy controls are necessary. The argument centers on what constitutes the smallest secrecy system that can effectively meet the security objectives. Because no policy can eliminate all miscategorized information, the tradeoffs concern the size and type of inherent errors. An expansive definition has obvious social and economic costs, but because secrecy also keeps information out of the hands of authorized people, it introduces a national security cost as well.[4] A definition that underprotects information clearly creates national security problems but increasing technology transfer might have important social and economic costs.[5]

9.1.4 Economic vs. National Security

Secrecy is generally viewed as having a negative impact on U.S. economic strength. Critics cite such economic impacts as the estimated $14 billion the classification system cost U.S. business[6] in 1989, the billions that export control costs through lost exports and additional overhead expenses, and the slowing of technological advances caused by the restrictions on scientific communication. Secrecy does not need to be entirely detrimental to economic health but may provide some benefits to commercial interests through technology conversion, protection of commercial information, and technology transfer restrictions. Analogous to the problems of restrictions on scientific communication is the tension over the terms of patents and copyrights, such as between the monopoly conferred by them and the antimonopoly thrust of antitrust statues.

The tension between national security and economic competitiveness will continue. Both represent fundamental objectives that must be supported. No guidelines exist to help politicians determine the relative weight each should be given. Wrong decisions can have serious consequences. Critics believe that giving too much consideration to military interests, as they believe happened in the Cold War, is counterproductive, because it unnecessarily weakens U.S. economic competitiveness, hence overall national security. Others say that giving too great an emphasis to economic interests will lead to a weakened military that cannot protect the country. Specific tradeoffs, as they arise, are probably best addressed on a case-by-case basis.

9.1.5 Civil Liberties vs. National Security

A large percentage of the public has lost confidence in government's trustworthiness in the area of national security. Some believe that the government is so obsessed with national security and related responsibilities, like law enforcement, that it willingly sacrifices every other national objective in the name of increased security. These people oppose every new secrecy initiative, such as the introduction of the Clipper chip, because of the potential—and for malicious disregard of the law—for a government conspiracy to violate the rights of U.S. citizens. There is a degree of truth in these assertions. Instances of past abuse[7] and deception[8] by the government support the proposition that the government sometimes acts maliciously. Countering that perception is the post-Cold War trend away from secrecy and toward greater openness evident in the shrinking export control list and increased openness of the CIA.

The Clipper chip illustrates the problem. When the government announced the chip as a tradeoff between commercial cryptographic needs and law enforcement requirements, most arguments were based on distrust of the government's intent rather than on the technical merits of the cryptography[9] or the need for wiretaps. Critics argued that the proposal should be rejected, because the government might abuse the ability to conduct wiretapping in order to conduct wide-scale spying on citizens and the eventual outlawing of other types of encryption. Issues such as classification and export control offer similar examples of distrust. Legitimate tensions will always exist between national security and civil liberties, and any policy must address both requirements.

9.1.6 Accountability

One factor leading to widespread distrust of government policy is a lack of accountability in the development of the secrecy system. Because of security, or a government claim of security, secrecy policies are not publicly debated, so that the public is left uncertain about the motives of the government and about whether the policy represents the best possible compromise. Although some policies, such as export control, receive limited debate through the legislative process, many secrecy policies, such as classification or cryptography, are implemented through presidential directives which bypass public scrutiny entirely.

Although the hidden development of secrecy policies is necessary to protect national security information used in the process, it also is useful to shield an administration from political fallout from the policy. The policies usually are released as take-it-or-leave-it propositions, with little or no stated rationale for them. The danger of this approach is that advocates for competing interests might frame public debate to support their own interests. The government, restricted by security and political considerations, often cannot or does not want to respond, thus conceding the public debate to the vocal advocates. Its refusal to answer seemingly important and relevant questions makes it appear as if not accountable or responsive to the people. Policymakers must balance security and political concerns with the need to provide enough information to gain public acceptance.

9.1.7 Foreign Relationships

Secrecy policies display a U.S.-centric position in regard to foreign availability of technology. The policies often appear based on the idea that U.S. technology and technology controls are unique and that unilateral mechanisms, such as extraterritorial export controls, provide adequate protection. Unlike the dominant economic position the U.S. enjoyed in the 1950s, in the early 1990s it has effective unilateral control over only a small amount of technology. Worse, technology developed outside the U.S., such as Japanese semiconductors or Russian satellites, is independent of any controls it imposes. Foreign countries can provide most commercial technology and much advanced military technology with their own economic and national security objectives. U.S. cooperation with multinational organizations like COCOM is necessary to achieve international protection. Any secrecy policy must consider the forms of foreign cooperation necessary to meet U.S. objectives and the level of cooperation attainable.

Areas of foreign availability that affects U.S. policies include, for example, export control, where foreign availability is an explicit consideration in licenses; foreign investment, where foreign availability of the germane technology is a consideration in allowing an investment; commercial satellites, where foreign satellites have better resolution than the U.S. permits; and commercial cryptography.

The tradeoffs in foreign availability and technology controls are not appealing. In such areas as export control, where unilateral controls can be thwarted by other countries, mutual security objectives need to developed through multilateral agreements like COCOM. The danger in extending a multilateral approach too far is that the resultant policy might be limited to the minimum agreeable objectives of the group and might not completely meet the requirements of the U.S. Ignoring international agreements and insisting on a unilateral policy that meets all the objectives of the U.S. would bring about national security and economic damage when other countries in their turn ignore U.S. controls. A delicate balance is necessary between ceding too many national security objectives to obtain international cooperation and making U.S. controls so tight that they alienate other countries into noncompliance.

9.1.8 Suppression of Technological Changes

The government seems to prefer to deal with advancing technology by controlling or suppressing it, regardless of practicality or possible consequences. Alternatively, the government could use improving technology to adapt old techniques or to invent new methods of achieving its objectives, as when the invention of the telephone enabled advances in law enforcement through wiretapping. Because rapid advances in technology increasingly undercut the government's ability to implement secrecy in the current fashion, the choice between suppression or adaptation to technology is not hypothetical. **Table 9-2** shows some tradeoffs involved in responding to new technology. National security objectives by their very nature reflect changes in technology. Nonproliferation underscores this idea. The original objective of the Cold War was to delay the spread of scientific information about weapons of mass destruction. Once that knowledge became widely available, the objective expanded to regulating the flow of raw materials and manufacturing equipment.

Table 9-2

Tradeoffs on Technology Restrictions

- Short-term ability to control technology
- Length of time technology can be suppressed
- Time necessary to develop new techniques
- Long-term loss of economic competitiveness
- Consequences of inevitable failure of controls
- Inability to control foreign development of the technology
- Inability of the government to control commercial growth of a suppressed technology

The government would like to frame the argument over the proper form of technology growth, because unregulated growth might cause it to lose its ability to meet national security objectives. This argument includes such examples as commercial cryptography, the need for tight export controls on computers and telecommunications equipment, and the need to limit the technology used in commercial photographic satellites. Although controlling technology may, in the short run, meet critical security objectives, long-term prospects are not good. Commercial technology continues to advance in unforeseen and potentially damaging ways that may eventually overwhelm government controls. Supercomputer technology, subject to export control, illustrates the problem: computers that use numerous parallel small computers, which themselves are not subject to export control, are advancing at such a rate that traditional supercomputers may soon be replaced by them. Government controls that target the speed of individual processors will be useless, and the issues associated with the export of supercomputers, such as diverting computers to work on military problems, will only spread. As a general rule, suppression or control of technology is at best a delaying tactic, though nonetheless worthwhile if used at the right time and for a limited time.

9.1.9 Implications of the Information Age

The foundation of the classification system was built by President Truman. COCOM started in the 1940s, and most of the secrecy laws, such as the Atomic Energy Act, were passed in the late 1940s. The structure these approaches reflect may no longer be appropriate

owing to major political, economic, conceptual, and technological changes of the last fifty years. Aside from the breakup of the former Soviet Union and the appearance of an integrated world economy, technology has shifted from the industrial age to the information age.[10]

During the industrial age the government believed information and technology could be controlled. Within the paradigm of that age many of the secrecy policies discussed in **Chapters Four** through **Eight** were effective. The paradigm of the information age is an explosion of information and a rapid turnover of commercial technology: information is more important, less controllable, and more widespread than mechanical technology. For example, advanced communication equipment prevents the government from controlling news reporting events except by restricting access, and the predictable result will be an increase in tension between the media and government. **Table 9-3** outlines differences between the industrial and the information age.

Many contemporary secrecy tensions and related tradeoffs resulted from the shift in paradigms. For example, because commercial technology turns over more quickly than export lists can be updated, the lists are filled with obsolete technology. In another, the explosion of information means that more people have access to potentially damaging information, which increases the required scope of control. Scope offers problems in the ambiguous nature of a large classification system, the detailed review necessary before foreign investment in defense firms can be allowed, and the potential for technology transfer through unrestricted scientific communication.

Any secrecy policy must adapt to the information age. Not all mechanisms available in the industrial age will be effective in the information age. Advancing technology rendered some impractical but may also provide new techniques, such as stronger computer security to protect information and allow some that previously was not protectable, such as government databases on private citizens, to be protected in the future. A practical policy would recognize the limitations and take advantage of the new possibilities inherent in the information age.

9.1.10 Problems in Government Implementations

The preceding chapters generally treat the government as a monolithic block that interprets and implements a consistent secrecy policy, which clearly is not true: internal

government squabbles over policy matters are endemic. Graham T. Allison's book on the Cuban missile crisis, *Essence of Decision* examines how interagency interactions affect policy.[11] Each agency has different objectives, such as providing national security or encouraging economic development, and each is reluctant to do anything it perceives as weakening its own power base. Policy differences between the executive agencies and Congress also must be considered. The result of unavoidable disagreements is contradictory and arbitrary implementation of policy.

Table 9-3

Shifting Paradigms Underlying Secrecy Policy

Industrial Age
• Wealth consisted of the U.S. industrial strength • Information and technology contributed to industrial strength • Information increased slowly • Communications were slow and limited in scope • The government controlled (or regulated) the communications infrastructure • Military strength translated into national security
Information Age
• Information has become a critical component of wealth • The amount of information doubles every ten years • Computers and satellites make cheap, instantaneous global communication possible without a government-controlled infrastructure • New forms of communications are evolving that will ease communication • Communications channels are virtually unregulated, increasing the difficulty of government control of information • Information and technology are critical aspects of national security: communications infrastructure is the first target of a modern army

The advantage of splitting policy responsibility among executive agencies is that it allows fuller discussion of relevant issues before a policy decision is reached. The disadvantages of diffuse responsibility include: dilution of responsibility so blame for an unworkable policy does not fall on any one agency, thus elimination of an incentive to find an acceptable compromise; compromise by the agencies on a vague definition that has a wide scope in order to meet every requirement; slowing development of an unfavorable policy through bureaucratic delay; interpretation of policy by each agency according to what best fits its individual objectives, in the absence of any central authority that would have power to implement policy consistently; and outdated policy, because no agency can modify policy in response to changing conditions. Even active presidential leadership is not always enough to overcome bureaucratic impediments to the development of policy. The declassification regulations promulgated by three successive presidents, for example, were routinely ignored by the implementing agencies through lax enforcement of them.

Although bureaucratic disagreements certainly are not unique to secrecy, they may have a greater impact there than usual. Deciding among competing interests of government agencies normally follows a political battle fought in public through authorized leaks and press conferences. The facts leading to the decision on a secrecy policy by their very nature must remain secret, which precludes the typical approach. Beyond strong public pressure, there are few ways to force implementation standards on individual agencies. Care is needed to formulate secrecy policy that will guard against adverse impacts of bureaucratic arguments.

9.1.11 Haphazard Development Process

Secrecy did not arise as a complete and consistent system arrived at as the conclusion of a well-thought-out decision process. It arose and is continually modified as a long series of individual decisions and precedents. As with any set of precedents, the process introduced many internal contradictions and omissions that distort the system, for example, the contrast in information about the defense and intelligence budgets. The DOD releases detailed breakdowns on troop size, troop deployment, weapons developments, and weapons purchases[12]; the intelligence community does not release even its composite budget[13] although various presidents and directors of the CIA[14] have supported releasing the budget and the Senate is authorized to release that information independently. These contradictions allow critics to argue that the secrecy system is fundamentally flawed and needs a complete

overhaul. The courts, which often resolve disputes like this in other areas of American life traditionally take a hands-off attitude toward secrecy. They refuse to resolve executive privilege cases, for example, and do not take advantage of their ability to conduct "in camera" review of classification decisions.

The secrecy system that started in the late 1940s was intended to cover an extremely wide scope, from a ban on exports to the Soviet Union to granting classification authorization to every government agency. The policy was narrowed through a series of case-by-case decisions, not a general philosophy regarding the kinds of information that needed protection. After factoring in bureaucratic inertia and the diffuse nature of the system, which keeps decisions at one agency hidden from other affected agencies, the accumulated inconsistencies are not surprising.

A strong central authority that would oversee secrecy policy might not be a better solution. Classification and declassification are local decisions, but because many agencies handle similar information, the possibility of inconsistency is large. For a central authority to ensure consistent classification decisions across these agencies, much information would need to be exchanged between agencies to outline decisions and a process to settle disputes between agencies would need to be developed. A central authority with these responsibilities would quickly become an unworkable bureaucracy. A complete, consistent secrecy system appears out of reach, and discrepancies will have to be tolerated.

9.1.12 Interrelationships

Individual secrecy policies accomplish only limited national security objectives. All policies working together are necessary to accomplish the overall objectives. The close connection among the policies means change in one affects the others. Care must be taken when modifying one secrecy component so that the desired outcome is not undermined by unintended effects in another.

For example, classification underlies almost all other secrecy policies, and any change in the classification system has repercussions in the other areas. The basic secrecy definitions are often built on classified information and change when classification changes. Technology transfer restrictions depend explicitly on classification. Export control has a munitions list,

which consists largely of classified technology, and a dual-use list of unclassified commercial technology, which has different restrictions. Generally, unclassified technology can be transferred to private industry, and defense firms can use unclassified technology in commercial products. Changing ideas about classification would also influence the perception of the government in regard to civil liberties. Tighter classification regulations could prevent many abuses—such as classification for political purposes or the use of classification to hide details of national security questions—which could cause distrust of the government.

As another example, repercussions of export control extend beyond specific products controlled, because it also affects other technology transfer policies. Commercialization of technology possibly subject to export control is sometimes difficult, because the controls give the government indirect control of a range of technologies that might be attractive to industry. Military technologies with civilian uses, such as photographic satellites and commercial cryptography, are controlled by the government through export regulations. The added expense of export control administration and the possibility of limited markets make many companies shy away from export-controlled technologies. Some changes in secrecy policy that affect other policies are shown in **Table 9-4**:

Table 9-4

Relationships of Secrecy Policies

Classification	**National Security Technology**
• Technology transfer • Export control • Flow of public information	• Flow of public information • Export control • Foreign direct investment policy
Export Control	**Flow of Public Information**
• Foreign direct investment policy • Foreign military sales • Technology transfer	• Privacy Act • Freedom of Information Act

9.2 Effects of Secrecy

The historical forces that motivate secrecy appear to be declining slightly in the post-Cold War environment. The challenges that face the country have begun to shift from primarily a superpower military standoff to an eclectic combination of interrelated military, economic, and social problems. As the mission of the military expands from protection against military attack into such areas as drug interdiction and humanitarian relief, the wall that once separated the national security community from the rest of society is cracking just a little. This shift allows the sacred cows of the security establishment, like secrecy, to be reevaluated for continued relevance and priority. Not surprisingly, the call for less secrecy can be heard like a siren song from many senior government officials convinced that would help solve many of this country's problems.[15] Among the benefits claimed for it are that it would stimulate economic growth and begin to restore people's confidence in government without hurting essential national security missions.

Secrecy has important economic and social costs. It hurts the economy through direct costs, such as those needed to run the classification system or through lost sales caused by export control but probably even more through indirect impact on technology and technology development. Social costs are reflected in distrust of government owing to the perceived violation of other constitutional rights in the name of national security. Secrecy is seen to have a negative impact on free speech, the public right to know, privacy, and economic rights.

These social and economic costs translate directly into national security problems. The direct expenditures to operate the security system take away valuable resources, especially with a declining defense budget, that could be used to support soldiers or weapons. Any decline in technology development adversely affects national security because the military depends on high technology to fight wars. Public opinion affects the way the military can conduct conflicts, as was highlighted in Vietnam. During military conflicts, when society most needs to rally round the government, distrust causes people to doubt the government and can shatter the necessary cohesion.

Secrecy exists, however, because it is necessary to the country. The national security community, as well as other agencies such as law enforcement, need secrecy to operate. U.S.

lives are at stake. Unnecessary openness about the intelligence community, military plans, military technology, or law enforcement investigations could cost lives in the next conflict.[16] Secrecy also provides economic benefits through reduced defense budgets. Given that for national security the U.S. needs at least a minimum level of military advantage over the rest of the world, increased openness might allow other countries to close the gap and require higher U.S. defense budgets to maintain an advantage.[17] Because the post-Cold War world situation has not eliminated the dangers of military conflict and because national security will need to remain a high-ranking national priority for the foreseeable future, secrecy in some form will remain necessary.

As this paper attempts to show, the tradeoffs involved in the secrecy system are more complex than what simplistic truths—such as less secrecy equals improved economic competitiveness—might convey. Decisions about the proper role of secrecy require a balance of several different societal needs. Such questions as how much increased economic competitiveness is worth how large an increase in national security risk must be addressed. Because secrecy mechanisms are interrelated, apparently simple decisions in one area produces a domino effect that influences similar questions in many others. Secrecy in its varied forms brings both benefits and costs, and the optimal mix of mechanisms differs depending on the interests of each observer and the prevailing circumstances. All stakeholders cannot be satisfied, so no matter what final policy emerges from ongoing reviews, secrecy will remain a contentious subject, that needs constant review to ensure a balance that best reflects the ever shifting priorities of society.

Notes

1. See Gary T. Marx, "To Tap or Not to Tap," *Communications of the ACM*, **36**, 3 (March 1993), 41.

2. To illustrate the usual manner of this argument, the Presidential Release announcing the introduction of the Clipper chip discussed commercial cryptography and law enforcement needs as follows: "There is a false 'tension' created in the assessment that this issue is an 'either-or' proposition." Statement by the White House Press Secretary, April 16, 1993.

3. President Bush, *National Security Strategy of the United States*, 3-4.

4. Two examples of military problems caused by excessive secrecy are the planning for the hostage rescue mission to Teheran and the invasion of Grenada. Planning for both operations was hampered by restriction of information from important elements that might have contributed. Black programs routinely keep technology away from people and defense organizations who could benefit from the knowledge.

5. The release of government information through a very strict reading of the privacy exemptions of the FIOA could result in loss of individual privacy. Premature release of U.S. technology could result in increased foreign competition.

6. Aftergood, "The Perils of Government Secrecy," 81.

7. Some well-known examples of abuse by government include Watergate, Iran-Contra, military drug experiments, intelligence agency abuses uncovered by the Church committee, and the illegal wiretapping of Martin Luther King, Jr.

8. The use of deception by the government as an adjunct to secrecy has a long and illustrious history. Deception can take many forms, such as outright lying—as when President Eisenhower said that the U-2 plane shot down by the Russians was a weather balloon—to providing misleading information to the public (the media)—as in the coverage of training for an amphibious assault on Kuwait.

9. *The RISKS-Forum Digest* (vol. 14) offers an extensive sample of the debate, two in particular by Eric S. Raymond and Marc Rotenberg. According to Raymond: "I believe that Ms. Denning remarked must be understood as part of a continuing propaganda campaign to marginalize and demonize advocates of electronic privacy rights. . . . These form a continuing pattern of attempts by agencies of the U.S. government to pre-empt efforts to extend First and Fourth Amendment privacy protections. . . . One of the traits of this culture of control is the belief that manipulative lying and dissemblage can be justified for a "higher good". . . . It is important for us to recognize that the propaganda lie is not an aberration, but a routine tool of the authoritarian mindset. . . . We cannot trust representatives of an institutional culture that was *constructed* to deal in information control, lies, secrecy, paranoia and deception to tell us the truth" (Number 64, May 19, 1993).

According to Rotenberg, Washington Director of CPSR: "One of the reasons for the concern was the secrecy surrounding the development of the standard. The documents disclosed by NIST and NSA to CPSR make clear the NSA used its classification authority to frustrate the attempt of even NIST's scientists to assess the candidate algorithm. This is not part of 'normal practice.' In fact, NSA's efforts to blindfold NIST and the secrecy surrounding the process violated the central intent of the Computer Security Act, the very law that governs the relationship between NIST and NSA" (Number 62, May 17, 1993).

10. An excellent description of the implications of the information age is can be found in Walter B. Wriston, *The Twilight of Sovereignty* (N.Y.: Scribner's, 1992).

11. Graham T. Allison, *Essence of Decision* (Boston: Little, Brown, 1971).

12. Gordon Adams, "The Role of Defense Budgets in Civil-Military Relations," 15,17. "What is striking about the role of elected legislators in the defense budget process is the staggering volume of information they receive on the budget. . . . This transparency of information about the defense budget influences both civilian and military participants in the process. Military planners know their requests must make some sense to the ordinary taxpayer who will read about them in the newspaper. Members of Congress know they cannot lobby for favored weapons projects in total secrecy."

13. Steven Aftergood, "CIA Increases Intelligence Budget Secrecy," *Secrecy & Government Bulletin*, 12, July 1992, 1.

14. Supporters of releasing the composite intelligence budget have included President Carter and Director of Central Intelligence Stansfield Turner. The primary opposition centered on the fear that if the release of the information, although it is not in itself very sensitive, would lead to pressure to release more sensitive information about the intelligence community's budget. U.S. Congress. Senate. Select Committee on Intelligence, *Whether Disclosure of Funds Authorized for Intelligence Activities Is in the Public Interest*, 95th Cong., 1st sess., 4-5.

15. Among those calling for less secrecy are Senator Daniel Patrick Moynihan and DCI Robert Gates. Senator Moynihan said, "A Democratic president (Republican also) could do no greater service to the nation and to his administration than to set about an energetic, determined, *public* dismantling of the secrecy system" (Moynihan, "End the 'Torment of Secrecy,'" *The National Interest*, 27 [Spring 1992], 19). Gates said, "It concluded that in today's world CIA had to be more forthcoming in public about its mission and roles, the intelligence process and to the extent possible the way we go about our business." Gates, "Statement on Change in CIA and the Intelligence Community," April 1, 1992, 16.

16. The raid on the Branch Dividians in Waco, Texas, offers an extreme example. The members of the cult were warned in advance that the ATF agents intended to raid the compound. Four federal agents died in the shootout.

17. THE DOD explicitly argued this point in the area of export control; according to the DOD, export control provided a net economic advantage to the country. The cost of export control to industry was less than the increased defense budget necessary to counteract the exports.

Acronyms

ACLU	American Civil Liberties Union
AEA	Atomic Energy Act
AFCEA	Air Force Communications and Electronics Association
BNL	Banco Nazionale del Lavoro
CBEMA	Computer Business Equipment Manufacturers Association
CCL	Commodities Control List
CFIUS	Committee on Foreign Investment in the United States
CIA	Central Intelligence Agency
COCOM	Coordination Committee on Multilateral Export Controls
CPSR	Computer Professionals for Social Responsibility
CRADA	Cooperative Research and Development Agreement
DES	Digital Encryption Standard
DOD	Department of Defense
DOE	Department of Energy
DSS	Digital Signature Standard
EAA	Export Administration Act
EAR	Export Administration Regulations
E.O.	Executive Order
EPCI	Enhanced Proliferation Control Initiative
FBI	Federal Bureau of Investigation
FDI	Foreign Direct Investment
FMS	Foreign Military Sales
FOCI	Foreign Owned, Controlled, or Influenced
FOIA	Freedom of Information Act
GAO	General Accounting Office
IAEA	International Atomic Energy Agency
ISOO	Information Security Oversight Office
ITAR	International Traffic in Arms Regulations
MCTL	Military Critical Technology List
MECEAA	Multilateral Export Control Enhanced Amendment Act
NAS	National Academy of Science
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NBS	National Bureau of Standards
NIST	National Institute of Standards and Technology
NRO	National Reconnaissance Office

NSA	National Security Agency
NSC	National Security Council
NSDD	National Security Decision Directive
NSF	National Science Foundation
NTIA	National Telecommunications and Information Administration
NTIS	National Telecommunications Information System
NTISSP	National Telecommunication and Information Systems Security Policy
OMB	Office of Management and Budget
OTA	Office of Technical Assessment
PD/NSC	Presidential Directive/National Security Council
PL	Public Law
Stat	Statute
USC	United States Code
USCIB	United States Council for International Business
USTR	United States Trade Representative