AD/A-006 901

# NEW APPLICATIONS FOR ARPANET DEVELOPED INFORMATION PROCESSING TECHNOLOGY. VOLUME II. SECURITY IN THE AUTOMATED PROCUREMENT PROCESS; SECRECY VERSUS EFFICIENCY: A LEGAL ANALYSIS

CABLEDATA ASSOCIATES, INCORPORATED

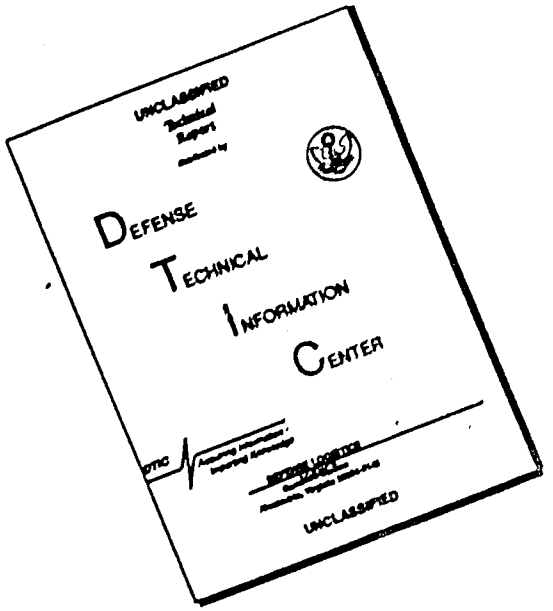
PREPARED FOR
ADVANCED RESEARCH PROJECTS AGENCY
AIR FORCE EASTERN TEST RANGE

3 FEBRUARY 1975

DISTRIBUTED BY:

NTIS
National Technical Information Service
U. S. DEPARTMENT OF COMMERCE

# DISCLAIMER NOTICE




THIS DOCUMENT IS BEST QUALITY AVAILABLE. THE COPY FURNISHED TO DTIC CONTAINED A SIGNIFICANT NUMBER OF PAGES WHICH DO NOT REPRODUCE LEGIBLY.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

| REPORT DOCUMENTATION PAGE | | READ INSTRUCTIONS BEFORE COMPLETING FORM |
|---|---|---|
| 1. REPORT NUMBER<br>R-171 | 2. GOVT ACCESSION NO. | 3. RECIPIENT'S CATALOG NUMBER<br>AD/A-006 901 |
| 4. TITLE (and Subtitle) NEW APPLICATIONS FOR ARPANET DEVELOPED INFORMATION PROCESSING TECHNOLOGY -- VOLUME II; "SECURITY IN THE AUTOMATED PROCUREMENT PROCESS; SECRECY VERSUS EFFICIENCY: A LEGAL ANALYSIS" | | 5. TYPE OF REPORT & PERIOD COVERED<br>Final Report<br>February 1974 - January 1975<br>6. PERFORMING ORG. REPORT NUMBER |
| 7. AUTHOR(s)<br>Cabledata Associates Staff in consultation with Paul Goldstein | | 8. CONTRACT OR GRANT NUMBER(s)<br>F08606-74-C-0043 |
| 9. PERFORMING ORGANIZATION NAME AND ADDRESS<br>Cabledata Associates, Inc.<br>701 Welch Road<br>Palo Alto, CA 94304 | | 10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS<br>PROGRAM CODE # 4P10<br>ARPA Order 2317/2 |
| 11. CONTROLLING OFFICE NAME AND ADDRESS<br>Advanced Research Projects Agency<br>1400 Wilson Boulevard<br>Arlington, VA 22209 | | 12. REPORT DATE<br>3 February 1975<br>13. NUMBER OF PAGES<br>59 |
| 14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)<br>Range Measurements Laboratory (ENL)<br>Air Force Eastern Test Range (AFSC)<br>Patrick Air Force Base, FL 32925 | | 15. SECURITY CLASS. (of this report)<br>UNCLASSIFIED<br>15a. DECLASSIFICATION/DOWNGRADING SCHEDULE |

16. DISTRIBUTION STATEMENT (of this Report)

Distribution unlimited. Available from National Technical Information Service, Springfield, VA 22151

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

---

PRICES SUBJECT TO CHANGE

18. SUPPLEMENTARY NOTES

---



19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Procurement, Computer Networks, National Security, Secrecy Act, Security Classifications, Computer Secrecy, Trade Secrets, Freedom of Information Act, Secrecy, Proprietary Data, First Amendment Limits to Personal Secrecy Agreements, Procurement Automation, ARPANET, Communications, Information Systems.

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

Discusses the tradeoffs in protection of information in an automated procurement system, in terms of costs and benefits to the government and to society at large. Also examines the alternative policy of increased openness and its security benefits-costs.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 68 IS OBSOLETE I UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

## PREFACE

An important question raised by the proposed procurement automation system is that of secrecy and national security. The procurement automation system of the future will necessarily contain a considerable amount of information. Some of this information in the past was classified, while much of the remainder had distribution by limited manual processes of filing and retrieval. With automation and easy retrieval, the issue naturally exists as to the degree that this information should be protected. Any protection from a foreign enemy ordinarily requires secrecy. This prevents our own citizens from using the information as well. Where shall the balance be?

This volume addresses the decision to secrete information in terms of costs and benefits to society. Denying a potential enemy information by secrecy raises the cost to him of reconstructing it. To the extent that resources which would have been used for harm are diverted to the task of reconstruction, the country possessing the information benefits. However, secrecy also raises the cost at home, and so denies the society of the benefits which knowledge might bring. Furthermore, secrecy can impose less tangible costs on society if a policy of secrecy is seen as damaging to national goals.

The alternative policy -- open access -- is also examined. It is argued that in most cases openness will provide more security in benefit-cost terms than secrecy. Procurement automation, because it deals with information which is often available in similar but public form, may be such an area where greater openness would be in the public interest.

This is Volume II of the two-volume Final Report. The present volume provides background information useful to the preparation of the first one. We plan to supplement this Final Report with additional reports on relevant issues in the subject area. These are in preparation for possible later distribution.

Volume I, ON THE AUTOMATION OF THE PROCUREMENT PROCESS: PRESENT STATUS, FEASIBILITY FOR IMPROVEMENTS, PROPOSED NEXT STEPS AND PAYOFFS, reports findings of key areas studied under this contract. It shows that over $1 billion could conceivably be saved each year (primarily due to improved competition) by the application of information technology to large systems procurement. These savings can be achieved using known techniques and advanced systems. However, a prerequisite to their application is a commitment by DoD to automation of large procurements.

CONTENTS

# EXECUTIVE SUMMARY

## CONTENTS

This volume provides a basis for assessing the impact of a proposed automated defense procurement system upon national security secrecy policies and their related issues.

The section EFFICIENCY AND SECRECY describes the role of information management as a national security measure and presents an analysis of secrecy's limits as a security device.

The section LAW AND SECRECY examines the limited efficacy of legal rules in guarding secrecy in a general setting and in two specific contexts: the executive classification program and the espionage statutes.

## POLICY ISSUES

The central strategic consequence of the procurement automation effort proposed in Volume I is that systematizing access to information relevant to the procurement process can confer order, intelligibility and a consequently critical dimension upon a body of data presently in disarray. The policy questions considered are:

- o whether, thus ordered, this information ought to be subjected to attempts at secretion from the view of foreign rivals;
- o whether the limited efficacy of secrecy in these circumstances combined with the dangers entailed by rivals' access requires a decision that procurement not be automated in the first place; or,
- o whether, assuming secrecy's limits, the security costs associated with rivals' access are sufficiently low to be outweighed by the benefits for overall national security that will flow from automation's contribution to efficiency in the defense procurement process.

Thus, any plans for computer-based automation of Department of defense procurement activities must raise many of the structural and legal issues that characterize the modern environment for the management of national security information.

## EXCLUSIONS

In approaching the questions of law and security raised by procurement automation, this report draws on lessons learned in other national security contexts. These related areas of national security information will not, however, directly be considered. Among the topics thus excluded are:

1. Tactical and operational information;
2. War plans generally -- the location of underground missile sites, for example;
3. Specific strategic vulnerabilities;
4. Intelligence activities, including the identity and deployment of intelligence personnel and sources;
5. Files on individuals;
6. The conduct of international negotiations, particularly where secrecy may be essential to candid discussion unfettered by public comment and political diversion.

The strategic and political interests, and the technological capabilities at hand in any of these areas differ sufficiently from those involved in defense procurement to warrant quite different approaches.

## FREEDOM OF INFORMATION

Information management decisions must address the constraint that government attempts at sequestering information may be foredoomed in the future by this nation's commitment to democratic values. The sweep and form that this commitment has taken to openness is broadly based on constitutional, statutory and administrative interpretation. Individual and institutional expectations respecting access to information are rapidly rising. This commitment has led to a new situation. Vast quantities of data are in the public domain, and much that is now labeled as secret can be reconstructed from freely

accessible data. Efforts at secrecy to be fully effective today would have to reach unacceptably far into the public domain. Secretion of masses of publicly available data may no longer be possible under other than a totalitarian regime. If the public availability of these data makes secrecy respecting the remainder illusory, the question arises whether present attempts at secrecy in most procurement activities ought to be abandoned or reduced. The answer will depend of course upon the countervailing gain that abandonment would entail versus the loss.

## A TRADEOFF

The benefits that could be derived from the proposed increase of automation are described in Volume I. Over and above a very large tangible dollar saving are intangible benefits. In short, they translate not only in lower purchasing costs, but in an increased capacity to keep defense purchasing abreast of technical change. These gains appear to outweigh the security costs entailed by a rival's discovery of the information that is being stored on-line. The rival is put to some expense in obtaining this information. Although this expense will probably be less than that involved in reconstructing the information independently, the rival seems likely now to be engaging in precisely this sort of independent reconstruction. The real issue here is open access to databases where the loss of information to the adversary is less than the gain in effectiveness to ourselves.

## RECONSIDERATION OF SECRECY

Secrecy is sometimes viewed as an end itself. This report considers it only one of many means for securing national interests in defense-related information. Secrecy's effective role has been sharply reduced over recent years by:

1. Changes in the nature and quantity of defense-related information.
2. The development of techniques available to rivals for the analysis of facts and data underlying the information.

3. Emerging pressures, from the congress, the press and the public, for enlarged access to presently sequestered domains.

A basic proposition considered in this volume is whether the presumption generally advanced in support of secrecy -- that all sensitive material be secreted:

1. can be reversed under modern conditions without sacrificing the security interests at stake;

2. perhaps should be reversed to accommodate official and representative decisionmaking pressures; and,

3. may have to be reversed if the rival will be more effectively disabled by the dispersion of a mass of undigested information than by the secretion of its more intelligible derivatives.

# 1. EFFICIENCY AND SECRECY

## EXTERNAL THREATS V. DOMESTIC ECONOMIES

A nation's security depends upon its domestic as well as its foreign strategies. It depends not only on its capacity to anticipate and meet threats posed by rivals, but upon the ability to maintain economic stability and social tranquility within its borders. Increased efficiency in production and equity in the distribution of wealth are components of national security.

This section of this report considers the information secrecy aspects of the dual concerns, foreign and domestic. Both sectors incorporate information-gathering activities symmetrical in their operation. In foreign affairs, an intelligence apparatus collects and analyzes data concerning a rival's military and industrial preparedness and prevailing economic, political and social trends. In domestic affairs, an archival apparatus exists for collecting and analyzing precisely the same sorts of data -- military, industrial, economic, political, social -- as they relate to the nation's internal condition.[1]

One nation's domestic data are, of course, another nation's foreign data. And, policies affecting the collection and management of domestic data must respond dually to the interests in informed decisionmaking on internal affairs, and to the interest in protecting these domestic data from the view of foreign rivals. The policy question is complicated by the fact that these two interests frequently conflict, and by the less frequently perceived fact that the chief problem encountered in such activities is not scarcity of data, but often its abundance and resistance to ordering into intelligible form. Thus, as between foreign and domestic data available to it, a nation must apportion scarce resources for the analysis of

data and their reduction to intelligible form. This in turn suggests that each government possesses neither a monopoly nor even a first claim on analyses of data respecting its internal affairs.

This duality, in which policies affecting domestic data gathering must not only resist foreign appropriation, but also serve to inform domestic decisionmaking, forms the framework of the discussion here. The specific focus is automation of parts of the defense procurement processes:

1. Should such facilities be open (in the interests of better-informed bureaucracy and electorate)?

2. Or, should they be closed (in the interests of resisting foreign nations' intelligence efforts or, at least not subsidizing their efforts)?

3. Or, given the risks involved, should the facilities not be constructed in the first place?

## FACTS, DATA AND INFORMATION

### Definitions

It is helpful to this discussion to classify the subject matter of intelligence efforts as facts, data, or information.

Facts consist of events and physical elements, natural or man-made -- rainfall in a western mining town, a rally of Young Americans for Freedom, a new aircraft carrier.

Data are reflections of facts -- an almanac's tabulation of annual rainfall, a newspaper report on the number of people attending the YAF rally, specifications or a photograph of an aircraft carrier.

Information consists of the selective manipulation of typically bulky data into more terse, useful and informative syntheses -- a report, for example, by the United States Department of Agriculture aggregating nationwide rainfall totals, comparing present figures with trends of varying durations, and assessing implications for future agricultural productivity.

### Differential Access

A government may, to the extent that it believes that a particular decision warrants the expense, ascertain facts, collect data and assemble information to guide the decision. Individuals, firms

and other governments can observe the same facts, collect the same data, and assemble the same information. And, through these functions, they can approximate the substantive decisions reached by the first government, particularly if they know the amount and type of facts, data and information used by this government in its decision, and the method of decision employed. The decisionmaking government may at the same time increase the cost of these outsiders' efforts by sequestering facts over which it possesses control, for example, by keeping the aircraft carrier from public view, not aggregating or publishing data, and not assembling or publishing information. These elements may, if the interest in obtaining them justifies the higher cost of the search, be reconstructed by outsiders from other accessible sources: knowledge of berth size, quantity of paint used and number of brooms and mops requisitioned, may for example, contribute significantly to an appreciation of carrier size and capacities.

## TO CONCEAL OR NOT?

Managerial considerations -- whether or not to publish -- cannot realistically be confined to the facts, data and information immediately at hand for a given governmental decision. These elements will probably have counterparts available in some form from the public domain and hence will naturally resist secretion. If data and information relevant to a government decision are not available from one source, they can often be derived from others. There is a limitation to the scope of general publication of data and information to a government attempting to secrete the remainder. The phenomenon of redundancy comes into play in which secreted facts can be reconstructed from available related facts, data and information.[2]

## LIMITS TO PARTIAL SECRECY

The thrust of this volume is that in the context of defense related procurement information, secrecy occupies a far more limited role than may be commonly thought. It represents, at best, a cost advantage

to government. It presents only a cost to be borne by outsiders in independently reconstructing from observed facts and data the information secreted.

Two questions, not one, underlie decisions respecting secrecy in the management of data relevant to national security:

1. whether to collect and organize data and to confer informational qualities on them; and, if systemized,

2. whether to publish or secrete this information.

## THE DECISION TO RESTRICT ACCESS

The decision whether to restrict access to information management and retrieval systems as described in Volume I should be made to depend only in part upon a comparison of secrecy's costs to the nation, for example, in terms of impaired bureaucratic and democratic functions[3] -- and its presumed benefits -- the maintenance of strategic advantage over rivals. There is a hazard in resting the decision exclusively on the proposition that a government's efforts at secrecy can deprive a foreign rival from access to the secreted information.

The assumption that secrecy is an effective means for selectively and absolutely hiding facts, data and information from the view of foreign rivals will be considered further in this volume as will the alternative proposition that secrecy measures may operate only to increase the cost to the rival of obtaining access.

Several phenomena, some enmeshed in the nation's political traditions,[4] others the result of modern technologies, others intrinsic to information itself account for the significant quantity of facts, data and information that are within easy public reach. These will be shown to form the basis for independent reconstruction, at some cost, of secreted facts, data and information respecting the national defense position generally and, at the least, of the type of strategic information being considered in this volume. We limit ourselves to discussion of information concerning a nation's defensive and offensive capabilities, particularly as these are a function of weapons systems presently existing and to be adopted.

While it is in the nature of the subject -- and perhaps testimony to the relatively meager resources made available to researchers interested in the question -- that little can be said with certainty about the efficacy of the government's secrecy practices, some direct evidence, considered in the section immediately below, can be drawn from the literature. Indirect evidence is also available in the form of a comparison with private firm behavior respecting secret, proprietary data. This will be discussed in the following section.

## THE LIMITS OF SECRECY: A GENERAL VIEW

A nation can be expected to invest in the secretion of information an amount seen to be comparable to its essentiality. Similarly, a rival can be expected to devote corresponding expenditures to its discovery, through appropriation or independent reconstruction, whichever appears to cost less. The political and economic costs entailed by an effort at complete secretion of all facts, data and information from which some aspects of the national defense could be reconstructed suggests that a number of relevant elements will continue to be accessible from public domain sources. This generally weights the rival's cost assessment toward reconstruction and away from appropriation through espionage.

This speculation on the role of competing expenditures is confirmed by available direct and indirect evidence of foreign intelligence activity in the United States. One often-told, and probably representative, anecdote is illustrative:

> [Allen] Dulles's predecessor [at the C.I.A.], General Walter Bedell Smith, was so disturbed by the difficulty of maintaining secrecy that he planned a test of the degree of security of United States defense secrets. He commissioned the services of a group of college professors for several weeks in the summer, and provided them with a stack of published information from newspapers, congressional hearings and reports, and government press releases.

> Their assignment was to determine how accurate an appraisal of U.S. military power could be assembled by a foreign intelligence system utilizing the same sources. After a few weeks of analyzing the open literature, they produced a highly accurate estimate of American military strength. When the findings were shown to the President and other top officials, they were deemed so accurate that, according to Allen Dulles, 'The extra copies were ordered destroyed and the few copies that were retained were given a high classification.'[5]

Still more direct, though more readily disputable, evidence is present in the observation of a Soviet defector, "that the Soviet military attache's office in the United States is able to legally obtain 95% of the material useful for its intelligence objectives." He asserted that "in fact, 90% of an intelligence agent's time in any other country in the world would normally be consumed clandestinely obtaining information which is readily available in the United States through Government agencies or commercial publishing houses."[6]

The experience of the United States intelligence establishment in obtaining, from their probably more circumscribed public domain sources, critical information concerning foreign nations may also shed some light on the nature of foreign activities here. According to one study[7] (probably the definitive publicly available work on United States intelligence practices):

> A rough breakdown of the sources of United States national intelligence for most of the 1947-1967 period would indicate the following magnitudes with respect to sources and collectors:

| | percent |
|---|---|
| Clandestine operations, covert sources, and secret agents | 20 |
| Press, radio, tourists, published documents, and other standard sources | 25 |
| Routine reports, Department of State and other government agencies abroad | 25 |
| Military attaches accredited by foreign governments and from routine military operations | 30 |

This breakdown does not, it should be noted, correct for the probable redundancy among sources, with some of the material obtained through clandestine sources doubtless replicable from the more overt sources.

Present and emerging analytic and surveillance techniques promise to threaten still further the integrity of secreted information, either through easier, more sophisticated means for reconstruction of public domain sources or through appropriation through espionage of the secreted material itself. Advances in social science methodology contribute to more accurate, sophisticated techniques for extracting meaning from disparate facts and data. Computer-assisted content analysis, though now far from a fully accomplished technique, may in the future help glean information by separating wheat from chaff in presently abundant and unyielding sources. Surveillance by satellite and through other communications and analysis mechanisms may conduce to a like result.

Secrecy possesses no inviolable core. It is a function only of competing expenditures among rivals. One nation's investment in sequestering information only raises the cost of another's in obtaining or replicating it This is the policy question at stake. Though this does not resolve the issue, at least it can be posed clearly. Imagine a hypothetical rival nation, lacking access to a systematized defense procurement base of the sort considered in this paper. It must plan to counter this nation's defense capabilities in an ineffectual random way over time. It must spread different types of defense systems along the range of possible developments in this country. However, giving it access to a systematized base saves it the cost of randomizing. And, it enables it now to develop its own capabilities on the basis of specific assumptions about what this nation's offensive capability will be years into the future. As a practical matter, if the intelligence apparatus of the rival nation is already being operated at an economic scale, and if this apparatus is already producing information approximating in quality that to be conveyed by a

systematized base, and if the entire apparatus cannot be dismantled without unacceptable losses for other intelligence-gathering activities, then the cost advantage to be conveyed by open access to the information base may be very small or only illusory.

## THE LIMITS OF SECRECY: THE INDUSTRIAL MODEL

### Using an Industrial Secrets Model as a Parallel for Discussion

While much can be inferred about the limited value of secrecy in the area of strategic security, it is in the nature of the phenomenon that little can be publicly confirmed. Government's reluctance to expose the full workings of the secrecy enterprise provides only one obstacle to accurate evaluation. It is a fully subsidized operation and because its benefits can be compared only awkwardly with its dollar costs, national security resists attempts at measuring overall efficiency. Analysis might for this reason be more readily accomplished by considering comparable behavior in the private sector. Although empirical support is only slightly less sparse, the theory of the firm provides a helpful tool for constructing a model of behavior.

### Proprietary Data Compared to National Security Secrets

Secrecy in a firm's maintenance of proprietary data possesses some important conceptual resemblances to secrecy in a nation's maintenance of defense-related information. By withholding from competitors information respecting its manufacturing processes, employee compensation programs, and research and development and marketing plans, the firm is able to develop competitive advantages akin to a nation's strategic advantage. By discovering or replicating its competitor's secrets, the firm can, through activities not dissimilar to a nation's programs for gathering intelligence, increase its advantage. The firm, like the state, relies for secrecy upon legal, technical and organizational mechanisms. And, like the state, it suffers substantial competitive inroads on these attempts at secrecy. State secrets are endorsed for their perceived essentiality to the maintenance of a nation's defense position. Trade

secrets are endorsed for more subtle reasons. By allowing the firm protection of its proprietary data, it is thought, investment in business, and specifically in innovative techniques, will be encouraged, with consequent advantage for the nation's economic welfare.

## Efficacy of Secrecy

There is an inherent difficulty in assessments of the efficacy of firm attempts at secrecy. Firms may be curtailed in their secrecy practices by legal prescriptions encouraging competitors' access to trade secrets. And, if this is the case, care must be taken to distinguish between the extent to which secrecy can be maintained as a technical matter and the possibly more confined extent to which the law permits protection. It appears, however, that trade secret law generally cuts no farther into the domain of secrecy than would technically be possible anyway. Laws drawn more favorably to the interests of the trade secret proprietor would as a practical matter easily by circumvented by competitors. The point can be made through a brief review first of the ambit of trade secret protection, then of competitive behavior apart from the law's command.

## Limitation of Legal Protection of Trade Secrets

Law's role in protecting trade secrets suffers many of the same practical and conceptual limitations that apply to state secrets. The extent of these limits should be evident from a brief description of the law's embrace: for an action for appropriation to lie, the subject matter in dispute must be a trade secret. A trade secret is "any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it."[8] The defendant's appropriation must have been accomplished either through breach of confidence, the typical case, or some other improper means. These might include, for example, "fraudulent misrepresentations to induce disclosure,"

or "tapping of telephone wires, eavesdropping or other espionage."[9] Under this approach, secrecy must not only be rigorously proven,[10] but it must also be shown that the information being used by defendant was plaintiff's secret, and if so, that it was improperly obtained. Protection is foreclosed if plaintiff's information borders on common knowledge, or on knowledge easily replicable from public domain sources. The extent that defendant arrived at information through independent efforts -- from public domain sources or from an analysis of plaintiff's product or public activities -- can also foreclose protection.

Reverse Engineering Allowed

Trade secret proprietors do not have a blanket right against replication. Competitors are allowed independent efforts in the same direction. Competitors' reverse engineering of trade secrets is allowable. Under this approach, the competitor starts with the proprietor's finished product and is allowed to surmise the processes and ingredients used in making it. Trade secret law resolves, on the side of free access, two issues left open by the nation's espionage laws and to be considered below:

1. whether the prohibition extends to situations in which the information, though secret, is reconstructed by defendant from public domain sources; and

2. whether the prohibition extends where, though defendant has improperly appropriated the secret, the underlying subject matter is available from the public domain, as data or information.

Practical Limitations

Permission of independent discovery and reverse engineering aside, practical obstacles stand in the way of law's guarantee of secrecy. Litigation necessarily entails the disclosure, usually pre-trial, of the plaintiff's secret and, often, surrounding business and research and development practices. While protective orders can be fashioned restricting disclosure to defendant's attorneys, the exigencies of suit will limit the orders' effect. The clear possiblity exists that more advantage will be lost by suing than by

not suing and this exerts a powerful disincentive to pursuit of the legal remedy.[11] Criminal prosecutions, although authorized, are few, in part because of the extremely narrow formulation, probably in the interests of due process, of the conduct proscribed.[12]

Limitation of Remedies

The most that the trade secret claimant can hope to gain from suit is to have defendant placed in the position he would have occupied had he acted lawfully. Compensatory damages are the rule, attorneys' fees and punitive damages the exception. Thus, in the usual case, plaintiff's headstart will be monetized.[13] Under the generally applicable rule an injunction will run for only so long as the trade secret remains secret. It will be dissolved when the protected information enters the public domain, as through widespread reverse engineering, independent discovery or the issuance of a patent. Alternatively, the injunction's duration may be preset through judicial estimation of the time that it would take a competitor to reverse engineer or independently develop the information in suit.[14] And where, as is most frequently the case, the action is against a departing employee, problems of proof -- involving subtraction of the secret information taken from the general skills and knowledge the employee brought with him to the firm -- are compounded by limits on the extent to which courts will allow employee mobility to be restrained through trade secret injunctions or covenants not to compete.[15]

Business Intelligence

To the extent that secrecy is maintained within the firm, it seems more likely to be the product of informal organizational and technical mechanisms than of the presence of legal sanctions. And, to the extent that secrecy is eroded by competitors, it seems more likely to be through conduct that falls outside, not within the legal sanction. Reports of buccaneering industrial espionage that occasionally appear in the popular press illumine only a very narrow corner of otherwise legitimate efforts at gathering intelligence

from public domain sources. The firm must, to thrive, operate in the world, selling the goods and employing the marketing strategies whose underlying information it wishes to keep secret. It must as well buy raw materials, hire and fire personnel, raise capital and, if publicly held, report to its shareholders. If the firm's business planning involves rational and systematic decision-making, competitors, also fluent in decisionmaking techniques, may hope to piece together and fill in from entirely public sources, the firm's overall strategy.

One not unrepresentative example may give some flavor of the realized possibilities for intelligence gathering:

> ...in order to impress upon a corporate staff how much data they were revealing through their employment ads, a team was assigned for one month to follow the personnel ads placed by the firm. They then made a report to the firm of their estimation of what was going on. To the great surprise of the firm's leadership, not only were they quite accurate in almost all areas, but they spotted three problems in production and quality control that the top brass did not even know existed![16]

One general canvass of "useful sources for business intelligence" included publications ranging from *Aviation Daily*, *The California Institute of Technology Weekly Calendar*, and *Business Cycle Developments* to *The New York Times*, *Business Week* and *Dun's Review*; another bibliography, of periodicals containing information specifically relevant to the defense industry, listed 81 sources.[18] A review of the attitudes of business people toward varying forms of intelligence gathering illustrates the span of these activities (and, presumably, their relative acceptability to business leaders). Among the more acceptable steps involved a retailer sending someone to shop in a competitor's store to get product and pricing information (96% approval) and an oil company establishing a scout department to watch the drilling activities of competitors (71%); among the less acceptable activities were those involving a design engineer stealing the plans of a competitor's new model (4%) and a company planting confederates in a competitor's organization (2%).[19] Employee mobility must also contribute significantly to the leakage of secrets.

## Competitive Advantage Under Limited Secrecy Protection

Where legal and institutional mechanisms fail to guarantee secrecy, the firm need not suffer a competitive disadvantage. Even here competitors will be taxed with the cost of gathering the underlying intelligence. Where these mechanisms are effective, and secrecy maintained, the firm will be afforded some additional degree of headstart, measured by the time that it will take competitors to arrive at the information independently. If the firm can determine beforehand whether the information it is developing will fall into the secret, or nonsecret class it will invest in the development of information accordingly. In the case of nonsecret information, it will invest an amount equivalent to the intelligence gathering costs of competitors, adjusted for the probability that competitors will not make the effort. In the case of secret information, it will presumably invest an amount equivalent to the profits to be made during the headstart period, an amount that may, but need not, be equivalent to competitors' reverse engineering costs. In both cases, investment may be increased commensurate with the probability that patent protection will be available for the information developed.[20] In either case, there will, then, be some incentive to invest in the development of technical information. And for this reason it would be inappropriate to cite continued investment in this development as evidence that secrecy is being enjoyed; considerations encouraging investment will obtain notwithstanding a complete lack of secrecy.

## Patents, A Difference in the Model

One reason, perhaps, that the limit of secrecy's value to private investment in innovation has not always been appreciated may lie in the availability of patent protection, an alternative or adjunctive means for appropriating to the firm the values of its invention. And if, as appears, the competitive advantage conferred by secrecy is not unyielding, and is subject to erosion by competitor's expenditures on discovery, then the patent system's requirement that claimed subject matter be made public in return for the grant of 17 years' exclusive rights may be only an illusory exaction. Secrecy

would, in any event, be lost relatively soon after marketing. The implication for national security interests in defense-related information, where no counterpart to patent protection is available, may be that attempts at maintaining secrecy over time will only rarely reward the effort.

## CHANGES WROUGHT BY AN AUTOMATED PROCUREMENT SYSTEM

In the context of the proposed automated procurement system, one related, more narrow question remains: Whether or not public access to proprietary data submitted in connection with bidding and contract performance should be allowed.[21] Defense contractors may view secrecy as essential to their competitive advantage and might, unless subsidized, be deterred from communicating to the Department of Defense technical information developed by them and of advantage to other defense or private contractors. Or, they may be deterred from dealing with the Department altogether -- thus depriving it of important innovation. Or, they may be generally dissuaded from investing in the development of this information.

At the same time, while recognizing the significant values that would attach to continued secrecy for proprietary data, the Defense Science Board's Task Force on Secrecy was sensitive to secrecy's costs for general scientific advance. It observed, for example, that the nation's lead in microwave electronics and computer technology was greatly extended after the decision in 1946 to release the results of wartime research in these fields.[22] Disclosure, though it yields benefits, has its strategic costs. The data are also placed at the disposal of foreign powers. The decision made in the mid-1950's to declassify information respecting nuclear reactors accelerated research and development into their peaceful use not only in this country, but abroad as well.[23]

## 2. LAW AND SECRECY

### LIMITS TO THE APPLICABILITY OF LAW

#### Basis for Ineffectiveness

Law seems a flaccid instrument for the protection of defense-related information from access by foreign rivals. "Secrets," no matter how close, will in the nature of government probably be shared by two or more individuals, and will consequently be in some sense public. Perhaps more important, the data underlying the secret will have some counterpart in public domain sources from which the secret can be reconstructed. To the extent that the secret is closeted, its theft seems likely to be covert and less detectable. To the extent that the secret is vital, and the value of its theft or independent reconstruction high, law's deterrent effect is diminished. And while it may be only in increasing the cost to foreign rivals of obtaining defense-related information that legal rules can be counted a success, this increased cost is equally imposed on friends -- citizens, primarily -- as well as enemies. And, it may impede access by the former to a greater extent than it does the latter.

#### Can Laws Be Made to Work Here?

Law's inefficacy in shielding defense-related data might of course be attributed to its modest, certainly alterable design. Yet a serious question exists whether present legal rules could through amendment be expanded, practicably and consistent with due process, to cover situations presently excused. There is, for example, a practical question of definition -- whether information derived and replicable from public domain sources can properly and actionably be defined as secret -- and a question of proof, and consequently of due process -- whether an alleged appropriator retrieved information

from a secreted data base or obtained it independently from data in the public domain. Even beyond the present shape of legal rules and what due process would allow, is the question whether, given information's special qualities, and the nature of the interests to be protected, any legal mechanism could be adequate to the task.

This last point should be evident from the difference between the performance being required of law in this area and the performance expected in other areas where its effect seems less disputable. The classification system, regulating official and public access to secreted information, might for example be likened to legal systems designed to regulate official and public use of government's real and personal property. Because in the case of real and personal property the object of regulation is tangible and discrete, it is an easy matter to determine whether the government's ownership interest is being infringed. Where, on the other hand, an outsider is using information that is replicated in secret government files, the question exists whether it was obtained from the files or constructed independently. Even if the outsider's access to the files at some point can be shown, this does not definitively resolve the issue in the sense, say, that it might be resolved in the circumstances surrounding trespass to land or appropriation of a government pencil or paper clip.

Example: The Pentagon Papers Case

The difficulty of framing a legal predicate for secrecy in the circumstances, and the predicate's essential nature as a cost advantage, may also be evident from the government's strenuous attempts to introduce a property rationale into the prosecutions arising from the theft of the "Pentagon Papers." In one of the cases,[24] which aborted before decision, the defense prepared to answer the government's charges of theft, conversion and embezzlement by reconstructing the information in the subject documents from public domain sources.[25] In the other,[26] the government's attempt to rest its case in part on a theory of copyright in the papers was specifically eschewed by Justice Brennan, concurring in the Court's

*per curiam* opinion.[27] Because the difficulty seems intrinsic to the nature of information and of legal mechanisms, the proper question to be asked in approaching new systems for the management of defense-related information may not be, how should applicable laws be framed, but, rather, should laws be framed at all.

## THE BUSINESS OF GOVERNMENT

### Introduction

The business of government is subject to two antithetical interests respecting the management of defense-related information. First is the perceived interest in secreting information that bears critically on national security. Second is the interest in exposing this information to an audience of responsible individuals, in and out of government, sufficiently diverse to assure that the strategy decisions reached will be well informed. Some broader, cognate interests may also become involved. Interests in due process may require that secret information be placed at the disposal of private litigants, for instance, or interests in informed representative decision-making may require that the information be imparted to members of Congress.[28]

In the following section we consider law and secrecy in the context of broader public demands, and focus on the operation of the espionage statutes. No attempt is made to present a synthetic overview of federal laws on secrecy and security.[29] Rather, statutes and cases have been selected for exemplary ends, to demonstrate law's relative inefficiency in defining and maintaining secrecy.

### Three Viewpoints

The perceived consequences of government decisions to conceal defense-related information will differ with the vantage from which the practice is viewed. From the viewpoint of the official making the decision, the decision will probably appear fairly straightforward. All defense-related information will be secreted as an initial matter. And, some will later be selectively disclosed upon a showing that the public benefits attending disclosure outweigh its costs to the national security. From the viewpoint of the outsider to the system -- the

litigant, congressman, scholar or member of the press -- seeking disclosure, the requirement that he precisely identify the information sought may appear a cynical device, barring him from access altogether. To the intelligence official of a rival power, rules governing secretion, disclosure and the particularity with which documents sought to be disclosed must be identified may appear to be an interesting charade, for he will characteristically be more interested in a tip, a lead or other piece of information gleaned from public domain or covert sources than he will in any classified document.

All three views possess a large measure of reality and each confirms the pivotal but strategically inconsequential position of the requirement that, to initiate the decision whether or not to disclose, a petitioner must first identify the material sought with sufficient particularity to distinguish it from the mass of information, mostly classified, maintained by government. The requirement is pivotal because it means that petitioners unable to identify the material sought with sufficient precision -- or, more realistically, unwilling or unable to meet the cost that such preliminary definition would entail -- will be denied access to this information. The requirement appears to be without consequence for the national security because foreign rivals -- as against whom the system of secrecy is presumably directed -- would seem to be more concerned with knowing that some event occurred -- the information needed by a petitioner to identify a document with particularity -- than with its documentary explication -- the subject of the petition -- and, unable to obtain this threshold information within the system, will reconstruct it from sources outside the system -- public reports, official leaks or through espionage -- precisely the sources that petitioners will, if they can bear the cost, consult in order to identify with particularity the documents they desire.

This point may be illustrated for introductory purposes with an example drawn from the earlier discussion of a base for systematized access to defense procurement information. If procurement functions are systematized in approximately the fashion described, officials in the Department of Defense would be well placed to recognize, well

ahead of the event, the probability that a given contractor will be unable to perform on schedule or in compliance with contract standards. For some outside institution -- a newspaper, say -- to uncover facts sufficient to alert it to this probability, and to form a basis for identifying the matter specifically, would require a costly vigilance or serendipity. A foreign rival -- or domestic competitor of the erring contractor -- might have a greater interest in uncovering the initial information and, though it would presumably be put to the same expense in the discovery, would not be particularly interested in the documentary details and would for this reason entirely avoid resorting to administrative, judicial or legislative process aimed at permitting access to these details.[30] The general point is explored in this section through a consideration, first, of judicial and congressional access to secreted information, then of the executive classification system, and finally of the informal system of leaks.

## Security in the Balance

Disputes raising questions of judicial and legislative access to information secreted in the executive branch reveal two phenomena that characterize rules on accessibility to secreted information generally. First, the demand for access is subjected to a balancing between the type of information involved, with defense-related information receiving the greatest deference, and the nature of the interests represented by the demand, with evidentiary needs in the criminal process apparently enjoying the greatest weight. Second, the most critical events affecting access to information occur outside this balance, where information may have to be gathered through other than procedurally regular routes in order to identify the information demanded with the required specificity, and where the availability of these informal routes may largely defeat the legitimate purposes of executive secrecy programs.

### The Judicial Process

Two Supreme Court decisions, one involving a prosecution request

for access to non-defense information, the other a civil plaintiff's request for defense-related information, indicate the outer boundaries of the balance drawn in these cases and suggest, too, the implied requirement in all these cases that the individual making the request have some initial, independent access to the information being sought.

United States v. Nixon. In United States v. Nixon,[31] in which the President of the United States sought to quash a subpoena, issued at the instance of the U.S. Special Prosecutor, directing him to produce specified tape recordings and documents relating to conversations with advisors, the Court balanced two opposing constitutional interests, "a President's generalized interest in confidentiality," and the "right to the production of all evidence at a criminal trial,"[32] and concluded that where, as here, the asserted privilege "depends solely on the broad, undifferentiated claim of public interest in confidentiality of such conversations,"[33] the privilege must give way to the criminal process:

> Absent a claim of need to protect military, diplomatic or sensitive national security secrets, we find it difficult to accept the arguments that even the very important interest of confidentiality of presidential communications is significantly diminished by production of such materials for in camera inspection with all the protection that a district court will be obliged to provide.[34]

The extent of the Court's solicitude for defense-related information should be evident from its careful extension of primacy to a claim of need, rather than to the need alone; where this claim is colorable, further inquiry even in camera by the Court alone, will presumably be foreclosed.[35]

United States v. Reynolds. Emphatic deference to defense-related material also marks the Court's earlier decision in United States v. Reynolds,[36] an action under the Tort Claims Act brought by the widows of three civilian observers who had perished in the crash of an Air Force plane that had been testing secret electronic equipment. The government, formally asserting privilege, rejected plaintiffs' efforts at discovery of the Air Force's official accident investigation report and of the statements of the three surviving crew members and also

resisted the District Court's order "to produce documents in order that the Court might determine whether they contained privileged matter."[37] The district and circuit courts held against the government's assertion of privilege.[38]

The Supreme Court reversed. Likening the privilege against disclosure of state secrets to the privilege against self incrimination, the Court observed that the trial "court itself must determine whether the circumstances are appropriate for the claim of privilege, and yet do so without forcing disclosure of the very privilege it is designed to protect."

> In each case, the showing of necessity which is made will determine how far the courts will probe in satisfying the occasion for invoking the privilege is appropriate. Where there is a strong showing of necessity, the claim of privilege should not lightly be accepted, but even the most compelling necessity cannot overcome the claim of privilege if the court is ultimately satisfied that military secrets are at stake.[39]

The Court referred for this last point to Totten v. United States[40] in which, in an action to recover compensation for covert intelligence gathering services alleged to have been rendered by claimant's intestate under an 1861 contract with President Lincoln, the Court, ruling against claimant, observed that "The secrecy which such contracts impose precludes any action for their enforcement;"[41] in the characterization given by Reynolds, "the action was dismissed on the pleadings without ever reaching the question of evidence, since it was so obvious that the action should never prevail over the privilege."[42]

Discussion of the Cases. So far as they purport to protect national security interests in defense-related information these decisions seem to possess a primarily formal consequence. The procedural requirements of civil and criminal litigation, requiring that documents sought before trial be identified with particularity, necessarily imply that the litigants can obtain a good deal of knowledge about the information held in documentary form by adverse or third parties, and that the document itself is being sought not so much for its ability to convey additional information as for its probative weight, its tendency to confirm what is already known.

In United States v. Nixon, for example, the Special Prosecutor was able to identify the precise circumstances of the meetings for which tapes were sought -- "the time, place and persons present" -- from White House logs that had previously been delivered to him;[43] as to content,

> With respect to many of the tapes the Special Prosecutor offered the sworn testimony or statements of one or more of the participants in the conversations as to what was said at the time. As for the remainder of the tapes, the identity of the participants and the time and place of the conversations, taken in their total context, permit a rational inference that at least part of the conversations relate to the offenses charged in the indictment.[44]

The devastating political effect of the tapes' revelation (and the implications of these political effects for the nation's international position) should not be confused with any direct strategic impairment which, had there been one, would have materialized long before, from the information indirectly received. Similarly, in Totten, claimant apparently had enough knowledge on which to rest his pleadings -- the date the contract was made and the agreed upon obligation to gather military intelligence in the southern states. It is difficult to imagine what additional information, adduced at trial and after the war's close, would, though possibly embarrassing, operate to compromise the nation's defense position.

## SECRETS KEPT FROM CONGRESS

### Executive Branch Prerogatives

Executive withholding of information from Congress dates back to President Washington's administration,[45] and seems generally less effective than similar attempts at withholding information from litigants. One reason is that Congress and particularly congressional committees concerned with a specific area of executive conduct, is routinely entrusted with information more sensitive than courts commonly seem willing to handle. Members may, for example, receive classified information in confidence from executive departments seeking congressional support on matters affected by the information.[46]

Congress and its committees are in continued contact with the workings of the executive branch. Its members can be expected to develop a closer and broader understanding of these processes. And, they have an intimate, readily accessible knowledge of the facts needed as a basis for eliciting specific items of information. Yet, enough instances have occurred in which congressional committees have remained ignorant of executive-held information simply because their members did not know to ask the right questions of the officials testifying before them[47] to indicate that, in certain contexts at least, members of Congress may even be considered to occupy a less favorable position even than private litigants.

Reasons for Withholding Information

On principle, it may be important to distinguish between two possible, quite different, reasons for executive refusal to provide Congress with defense-related information. In one case, the information is digested, collated and readily at hand, and withholding is justified by the executive on the ground that disclosure would compromise national security. In the second case, while the executive may have access to some of the facts and data underlying the information requested, it has not analyzed these materials and consequently is in a position more closely comparable to that of the Congress, with no ready access to the intelligible information that may be derived from these sources. The issue in the first case can in part be resolved by legal mechanisms as, for example, in a requirement that the Department of Defense periodically disclose to the Defense Subcommittee of the House Appropriations Committee, a list of all contracts entered into involving more than $10,000. The issue in the second case must first be resolved as a budgetary matter -- as, for example, in a Department decision to invest in the automation of procurement activities, including information retrieval -- before the legal requirement -- periodic reporting on contract performance -- can properly be imposed.

## THE CLASSIFICATION SYSTEM

### Concept

The executive classification system represents one attempt at incorporating into an institutional framework the balance between interests in secrecy and access. Under the classification program, data developed and gathered by government may be placed in one of several classes, depending upon their degree of relevance to the national defense. Formal access to these data is restricted to individuals in the public and private sector who have been "cleared" for this purpose on the basis of both their "need to know" the information involved, and on the basis of their estimated "loyalty" to the United States government. Under the Industrial Security Clearance Program of the Department of Defense, for example, a clearance will be granted only upon a showing that it is "clearly consistent with the national interest,"[48] and will probably be denied upon a showing that the applicant has committed or attempted an act of treason, disclosed confidential information without authority, or violated security regulations.[49]

### History 1789-1917

One source of the modern classification system is a November 21, 1917 General Order from the American Expeditionary Force Headquarters establishing the first formal military system for secrecy through a three-tiered classification system -- "Secret," "Confidential," "For Official Circulation Only."[50] Another source lies in measures prescribed by Congress for the custody by executive departments not involved in military efforts of documents prepared in the course of their day-to-day operation: a variety of statutes, the first enacted in 1789,[51] and finally brought together in 1875, provided essentially that the "head of each Department is authorized to prescribe regulations ... for ... the custody, use, and preservation of the records, papers, and property appertaining to it."[52]

### History 1951-1974

During the Truman Administration, these two lines of development, military and nonmilitary, were first brought together to form an

integrated system for the management of sensitive information gathered within the executive branch. Executive Order 10,290,[53] issued in 1951, extended the classification system employed by the Departments of Defense, Army, Navy and Air Force to civilian departments and agencies and added a "Top Secret" classification -- covering information that, if disclosed, "would or could cause exceptionally grave danger to the national security" -- to the existing, Secret, Confidential, and Restricted categories. The Truman Order was soon modified by President Eisenhower's Executive Order 10,501[54] which sharply confined the sprawling system envisioned by its predecessor. With subsequent, minor modifications,[55] the Eisenhower Order formed the framework for classification until the issuance, in 1972, of President Nixon's Executive Order 11,652.[56]

Though aimed at cutting down the amount of material classified by narrowing the opportunities for classification and by providing for declassification, the Eisenhower program was widely criticized for its continued insulation of data that many, in and out of government, thought would better be unclassified. President Truman had promulgated Executive Order 10,290 in response to claims of information seepage. One study cited by the President asserted that 95% of "secret" government information was being reported in the nation's press.[57] Two decades later, a retired government classification expert testified that probably 99.5% of the Defense Department's classified information could be disclosed without harm to national security.[58] President Nixon's Order, 11,652, employed two techniques to limit the scope of classification: it shrunk still further the circle of departments and agencies with power to classify, and it sought to increase administrative review of classification behavior.[59]

## Declassification

### Scheduled Declassification

As part of its effort at trimming the scope of the classification program, President Nixon's Order also introduced an accelerated timetable and more stringent procedures for the declassification of sequestered information. Under the declassification timetable, not

considering allowable exceptions, two years is the longest period within which information is classified as Top Secret or Secret, and six years for Confidential. Information classified Top Secret is automatically downgraded to Secret after two years from the date of original classification, to Confidential after another two, and declassified after another six. Secret information is automatically downgraded to Confidential after two years and declassified after another six. And Confidential material is automatically declassified after six years from the date of its original classification.[60]

Exemptions From the Declassification Schedule

Allowable exemptions from this timetable are numerous. Exclusions are provided for, among other items, information that in the judgment of an official with Top Secret authority, discloses intelligence sources or methods or a "system, plan, installation, project or specific foreign relations matter the continuing protection of which is essential to the national security."[61] Information classified and exempted under the Nixon Order is to be automatically declassified after thirty years from the date of its classification, unless an appropriate official of the originating agency determines and demonstrates that continued classification is necessary to national security or the safety of some person.[62]

Public Access

The first opportunity for review at the instance of a government official or private citizen of material classified under the Nixon Order arises ten years after the date of classification.[63] If the material's originating department, which is charged to undertake the prescribed review, fails to perform the requested review, or acts adversely on the request, an appeal may be taken, first to a departmental committee,[64] and then to the Interagency Classification Review Committee.[65] A National Security Council directive issued under the Order provides for a data index system intended to systemize departmental and agency management of classified information and to facilitate declassification and public access to materials once declassified.[66]

Responsibility for reviewing the great bulk of materials classified prior to the Nixon Order has been vested in the Archivist of the United States and subjected to generally the same standards applicable to departmental review of material classified after the Order.[67]

Must Know What You Want to Know

The chief hurdle to citizen initiation of review of exempted materials after expiration of the mandated ten-year period would appear to lie in the requirement that the document sought be described in the request "with sufficient particularity" to enable identification. And, as a related matter, it must be retrievable "with only a reasonable amount of effort."[68] The knowledge necessary to identify the document with particularity -- knowledge for example, of the approximate date of the document's classification and the general nature of its subject matter -- would appear to imply enough knowledge about the document to deprive the portions of it that remain secreted of any strategic value. In any event, it appears not unlikely that the cost to the citizen of pursuing review will exceed that of the added independent research that might be necessary to discovery of the document's remaining strategically relevant elements. This is particularly true when this cost is augmented by the probability that the request will be denied, since due deference will be paid to the official decision requiring exemption.

What Is Really Protected

What the classification program is designed to secure, and what declassification will reveal are not then items of information vital to national security. These would have to have already been compromised by definition by the kind of knowledge specified as the predicate for mandatory review. Rather, it protects only documentation that, on a given date, some agency of the executive branch in fact took a certain course of action. The interests that are served by the declassification scheme are, then, primarily those that derive from confirmation, from the capacity, that is, to

ascribe conduct with certainty -- academic interests, for example, certain interests of the press and foreign propaganda interests. With respect to information critical to the national security, the most telling feature of the declassification program is the assumption of its "sufficient particularity requirement" that the public will, prior to declassification, possess a good deal of knowledge about presumably secret subject matter, knowledge that will, inexorably, leak through the system's informal operation.

## LEAKS

### Prosecution or Administrative Sanctions

The efficacy of the criminal sanction in maintaining the integrity of the classification program is difficult to assess. Criminal prosecutions for the disclosure to foreign nationals of classified and unclassified data related to the national defense are, though numerous, of possibly limited effect, a point to be pursued in the next section. Where disclosure has not been to foreign nationals, but rather to other government employees or the press, the government has generally refrained from prosecution -- the prosecution of Daniel Ellsberg for conveying classified documents to the *New York Times*, is the single exception -- and has relied instead on administrative sanctions from reprimand through dismissal.[69]

### Tendency to Overclassify and Tendency to Leak

There also seems to be an overriding reliance in these matters on administrative mechanisms. These mechanisms may help to explain two closely related, and apparently contradictory, phenomena respecting secrecy. First, because the classification program predicates secrecy, the natural inclination where decision could go either way is for the government official to exercise discretion in favor of classifying the document; reprimand or failure to be advanced in the hierarchy is avoided and the informing ethic of the program is maintained. At the same time, where administrative sanctions are least toothy, and where interests in personal advancement transcend those of institutional fidelity -- phenomena most likely to combine at the

higher levels of government -- the program is highly susceptible to leaks, to members of Congress, say, or of the press, for any of a variety of personal reasons. Many of the same bureaucratic forces that lead government officials to prefer secrecy to openness in the decision whether to classify data gathered within their departments may also incline them to the selective disclosure of this information.

## Information and Power

Information represents some particle of power, and self-serving leaks, probable in any bureaucracy, seem particularly likely to occur in a democratic setting where critical decisions are the product of any number of countervailing political pressures, and where the press, with its capacity to mobilize public opinion, is an important and valued avenue for the exertion of these pressures. While the daily newspaper, larded with reference to "officials" or "informed" sources may give ample evidence of the extent to which high level bureaucrats are leaking classified information, or information otherwise denominated secret, some brief indication here of the occasions for seepage may be useful.

## Leaks Used For Forming Public Opinion

The place of leaks -- the intentional disclosures of secret information -- within a purposeful and politically functional public information program has been accurately captured in the observations of one seasoned journalist:

> Without the use of 'secrets' there could be no adequate diplomatic, military, and political reporting of the kind our people take for granted, whether abroad or in Washington, and there could be no mature system of communication between the Government and the people ... We have been taught, particularly in the past generation of spy scares and Cold War, to think of secrets as <u>secrets</u> -- varying in their 'sensitivity' but uniformly essential to the private conduct of diplomatic and military affairs and somehow detrimental to the national interest if prematurely disclosed. By the standards of official Washington -- Government and press alike -- this is an antiquated, quaint, and

> romantic view. For practically everything that our Government does, plans, thinks, hears, and contemplates in the realms of foreign policy is stamped and treated as secret -- and then unraveled by that same Government, by the Congress, and by the press in one continuing round of professional and social contracts and cooperative and competitive exchanges of information.[70]

These observations suggest not only that the continuing flow of "secret" information to the press is an accepted prerequisite to an informed electorate -- as well, possibly, as a governmental device for shaping public opinion through the selective release of documents -- but that it is also an important tool for the shaping of government decision through other than the electoral process -- as a vehicle, for example, through which a government official may shape bureaucratic, and possibly presidential behavior.[71]

Leaks as Trial Balloon

Any number of governmental or personal motives may underlie leaks of secret information. An administration may, for example, facilitate publication of reports on the imminence of a possible decision in order to test domestic and foreign reactions before itself taking definitive action. An official who desires that such a decision not be effected may, at the earliest and most tentative stage of its consideration, disclose the possible decision, in its most drastic form, to the press, in the hope that this will precipitate adverse and overwhelming domestic or foreign reaction.[72]

Leaks for Generating Support

Varying estimates of the comparative military strength of the United States and its rivals may be leaked to generate congressional and public support for military budgets and for the proponent's favored weapons project. And, within the sometimes Byzantine world of military politics, one branch, seeking to gain support for some project from another branch, as against the opposition of a third branch, may leak adverse assessments prepared by the third branch of some program of the second branch.[73] Leaks may also occur in the

course of ordinary bureaucratic infighting -- in an official's attempt to enhance his own position or to subvert another's[74] -- or in the service of more principled objectives -- blowing the whistle on project mismanagement, or alerting the President and Congress to the error of reports reaching them through official channels, as, for example, was reported to have occurred in dispatches from Viet Nam during the early 1960's.[75]

Leaks as a Source of Retirement Income

Bureaucrats in this country, relatively more mobile than the professionally oriented bureaucrats of other countries,[76] may also be an important source of intended as well as inadvertent leaks. At the highest levels of government service where turnover is particularly frequent, the dissemination of classified material by departing officials is notably widespread and, indeed, one central economic consequence of the classification program may lie in the headstart that it gives these officials in the preparation of memoirs that can promise the public at least a handful of surprises. Thus, a letter from Dean Acheson to the co-author of a study on scholars' access to government documents is remarkable not so much for its defense of the former official's use of documents as an aid to memory -- "The memoranda taken at the time straightened out a sometimes involved sequence"[77] -- as for its bland assumption that former officials should be free to relate, whether from memory or record, events and conclusions that reside in classified material, and to which they have obtained access only by reason of their privileged, official position.

THE INTERESTS OF THE GOVERNED

Introduction

Where access to defense-related information maintained in the executive branch is gained not through the procedurally regular routes open to other branches of government and to the public, but rather by unannounced -- covert or overt -- appropriation, an entirely different set of legal rules and issues surrounding the

relationship between secrecy and security is engaged. One issue, underlying the classification program's operation, appears, however, to persist: because information is at stake, and because information is naturally replicable, attempts through law to distinguish legitimate from illegitimate uses of information are ineffective at best and wrongly focused at worst; no less than in the classification context, the law's greatest effect appears to lie in its inhibition of informed political debate.

The chief statutory implements for securing defense-related information against outside appropriation, 18 U.S.C. Sections 793, 794,[78] are labyrinthine, redundant and diffuse and suffer a number of ambiguities. Covert and overt activities, each possibly compromising the nation's security but to different degrees, and affecting the public interest in vitally different ways, are comprehended by a single formula.[79] Section 794(a), for example prohibits espionage in its classic form -- the delivery of defense-related information to any foreign government "with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation;" subsections 793(d) and (e) take essentially the same approach in proscribing the disclosure of defense-related information by persons with legitimate access or possession to those without, and the disclosure by those without legitimate access or possession "to any person not entitled to receive it," and formed the bases, respectively, for the prosecutions of Daniel Ellsberg[80] and the *New York Times*.[81]

The different issues of secrecy and security can be divided into those attending covert takings of defense-related information and those attending overt takings. In the case of covert approprations, the central problem has been definitional -- to define the prohibited subject matter in terms that will be both useful to the national security interest and adequate to the requirements of due process. The definitional problem exists in the case of overt takings as well, but is compounded there by serious questions concerning law's efficacy in guarding against this class of conduct.

Covert Acts

The major premise of Sections 793 and 794, that defense-related information should be secured, is the statutes' operative premise as well: for a taking to be actionable, the information taken need not be secret, but only must relate to "the national defense." Using the statutes' broad, underlying concern as an express element of the crime, and foresaking narrower, more easily administrable elements, the statutes could be interpreted to prohibit the transmission of material based on social and economic facts, data and information this is generally available, that is of use in contexts other than defense and, though sometimes only peripherally related to the national defense, that is nonetheless defense-related. This breadth notwithstanding, Congress has long repelled efforts to define the statutory term more specifically.[82]

United States v. Heine

While secrecy is nowhere in the statutes imposed as a limitation on "related to the national defense," the concept has inexorably worked its way into the decisions. Judge Learned Hand's opinion in United States v. Heine[83] is typical. The information there, organized by Heine into detailed reports on the domestic aviation industry for transmittal to Germany in 1940, had been gathered "from various sources: ordinary magazines, books and newspapers; technical catalogs, handbooks, and journals; correspondence with airplane manufacturers; consultation with one, Aldrich, who was already familiar with the industry; talks with one or two employees in airplane factories; exhibits, and attendants at the World's Fair in New York in the summer of 1940."[84] Holding that defendant's conduct was not covered by the statute, Hand reasoned, "it is obviously lawful to transmit any information about weapons and munitions of war which the services had themselves made public; and if that be true, we can see no warrant for making a distinction between such information and information which the services have never thought it necessary to withhold at all."[85]

The difficulty with Judge Hand's limitation lies only partially in his refusal to distinguish between information published by the armed services and "information which the services have never thought it necessary to withhold at all," between facts and data gathered and published by government and those not gathered, and in this sense possibly inaccessible to the United States government. Another part of the difficulty lies in the limitation's failure to resolve the situation in which the information, though indeed secreted within the military, was, as will often be the case, independently replicable from public domain sources. It is possible that for every analysis completed by Heine on the basis of public domain data, there was some substantial replica kept secret by the government and, while Judge Hand may nonetheless have excused this conduct, the propriety of such a result is not self-evident. Nor, for that matter, is it self-evident that Heine ought to have been convicted under the obverse situation -- where, though he had appropriated the secreted information, the information was nonetheless replicable from public domain sources. Hand's opinion gives little evidence of the result he would have reached in either of these sets of circumstances.

Gorin v. United States

Secrecy was earlier put to a different use by the Supreme Court in Gorin v. United States.[86] Recognizing, like the Second Circuit Court of Appeals, a need for more rigorously defining the concept of "related to the national defense," the Court found that the "obvious delimiting words in the statute are those requiring "intent or reason to believe that the information to be obtained is to be used to the injury of the United States, or to the advantage of any foreign nation,"[87] and reasoned that where "there is no occasion for secrecy, as with reports relating to national defense, published by authority of Congress or the military departments, there can, of course, in all likelihood be no reasonable intent to give an advantage to a foreign government."[88]

This asserted relationship between secrecy and scienter is surely a *non sequitur*, for situations will arise, as in United States v. New York Times, in which, though the information is secret the intent is more than colorably benign or, as in United States v. Heine, in which, though the information is public, the intent is malign. And, even accepting the Court's logic, attention is only shifted from the admittedly elusive element of intent to the no more tractable question of secrecy. As between the two elements -- the explicit requirement of scienter and the implied requirement of secrecy -- the first, shorn of any probative reliance on secrecy, seems the more appropriate and manageable: appropriate, because it introduces a generally applicable principle that does not depend for its operation on necessarily unsatisfactory definitions of secrecy, and manageable, if only because of its historic, well-elaborated function in the administration of criminal law.

## Overt Acts: Violation of the Espionage Statutes

### New York Times Co. v. United States

Definitional quandries attend the application of the espionage statutes to overt activities -- press reports of information related to the national defense, for example -- no less than to covert activities. There is additionally an important threshhold question whether, taken literally or in light of their legislative history, the espionage statutes embrace the publication, and conduct preparatory to publication, of defense-related information. The first definitional question has already been treated in the discussion of covert activities; the second has been exhaustively pursued elsewhere[89] and will not be further ventilated here. Consideration will focus instead on law's efficacy in maintaining secrecy against attempts, predominantly by the press, to subject secreted information to wide public scrutiny.

The facts and decision in New York Times Co. v. United States,[90] in which the government sought unsuccessfully to enjoin the *New York Times* and *Washington Post* from publishing the contents of a classified study, "History of U.S. Decision-Making Process on Viet Nam

Policy," illustrate two important limitations, and one possible prop, to law's operation in the area: the limitations stem from the first amendment's general inhibitions on prior restraint and, even assuming the legitimacy of the injunctive decree, from the law's failure effectively to guard secrecy under the circumstances. The possible doctrinal aid to law's efficacy lies in the distinction, not elaborated by the Court, between a government's authority to fetter press discussion -- the usual stuff of first amendment controversy -- and a quite different obligation, to turn sequestered information over to the press -- arguably the situation in New York Times.

The one point on which the New York Times majority agreed, that under the facts the government had not met the heavy burden of justifying prior restraint of the newspapers' publication of the Pentagon Papers, only barely intimates the extent to which the first amendment will compel sacrifices of secrecy in the face of press demands. It is impossible to divine from the several concurring opinions any majority agreement on the circumstances under which the government would be held to have discharged its burden: for one Justice an injunction would have been tolerable under only the most compelling conditions of individual peril;[91] for another, a specific congressional provision for the injunctive remedy might have been sufficient to tip the balance;[92] while for two others, prior restraint would apparently have been impermissible under any circumstances.[93] Also left unanswered was the question of the extent to which, though prior restraint would be prohibited, the criminal sanction, applied after publication, would be permitted, thus possibly deterring publication and effectively achieving the same result as prior restraint. At least three of the Justices, while outlawing prior restraints, would apparently have sanctioned post-publication prosecutions in the same circumstances, thus through deterrence erecting a second line of defense for governmental secrecy.

By fastening on the government's claims to secrecy and defendant's claims of privilege, the opinions generally overlooked that secrecy was not the issue in New York Times v. United States and that only rarely will it be an issue in cases of press publication.

*New York Times* reporters had evidently spent no less than three months analyzing the Pentagon Papers;[94] the papers were before publication subjected not only to their scrutiny, but to the attentions of editors, proofreaders and typographers of the *Times* and *Washington Post*. The group within which the papers circulated was probably larger and, more important, was unregulated by government security clearance procedures. To speak of information at this stage as secret, and to characterize the next step, publication, as entailing loss of secrecy, would deprive the term of any useful meaning.

The point, then, is that even were an injunction against publication to issue, even were prior restraints and post-publication prosecutions broadly tolerated, in these or other circumstances involving overt acts, their effect would not be to maintain secrecy -- for that would already have been lost through necessary pre-publication conduct -- but only to still debate. Legal regulation of secrecy, if it is to be effective at all, must focus on the control of government employees and others who, through covert acts, may enable overt disclosures.

A more persuasive case for government restraint might be rested on a distinction of the press' usual role -- reporting and commenting on facts, data and information gathered by it from the public domain -- from the role it played in New York Times -- appropriating facts, data and information assembled by the United States government. Professor Henkin has astutely observed:

> Doubtless, the [first] amendment sought to protect the freedom of the Press to report and to criticize the actions of Government. In publishing the Pentagon Papers the Press asserted something more -- the right to publish documents prepared by, belonging to, and emanating from the Executive Branch that, in the exercise of constitutional responsibility, the Executive sought to withhold. One can argue that the traditional freedom of the Press is not an issue, and that the Press is not free to publish confidential government documents with impunity, even less, say, than it could publish private documents in violation of a copyright, or disclose protected trade secrets, or invade individual privacy. But Government has a monopoly of masses of important information and it could effectively curtail the freedom of the Press to report and criticize by withholding that information, or distort the function of the Press by selective 'hand out.'[95]

The trade secret analogy is particularly instructive for, as discussed earlier,[96] trade secret law confers a "monopoly" in only the most limited sense, and it may well be that the government's "monopoly of masses of important information" is likewise comparatively thin, representing, at best, a cost advantage over the press, requiring it to reproduce independently from public domain sources facts and data held by the government as secret.

FIRST AMENDMENT LIMITS TO PERSONAL SECRECY AGREEMENTS

These last two extrapolations from New York Times Co. v. United States suggest that, to be at all effective in maintaining secrecy, legal mechanisms must join with social and technical mechanisms to safeguard information from covert appropriations, typically by government employees, and in dealing with press and other public appropriations, operate to buttress the economic advantage obtained through the government's fully subsidized assembly of critical information. The government's attempt to enforce a secrecy agreement executed by Victor Marchetti, a former employee of the CIA, represents an effort in the first direction.[97] The Freedom of Information Act[98] might appear to be an effort against the second.

As against the government's contract claim in Marchetti, defendant asserted that "his First Amendment rights foreclose any prior restraint upon him in carrying out his purpose to write and publish what he pleases about the Agency and its operations."[99] Holding against defendant, but without relying upon the doctrines developed to limit secrecy covenants widely employed in the private sector, the court ruled that "the First Amendment limits the extent to which the United States contractually or otherwise, may impose secrecy requirements upon its employees and enforce them with a system of prior censorship," but that while the amendment "precludes such restraints with respect to information which is unclassified or officially disclosed...we are here concerned with secret information touching upon the national defense and the conduct of national affairs..."[100] Consequently,

> Marchetti retains the right to speak and write about the CIA and its operations, and to criticize it as any other citizen may, but he may not disclose classified information obtained by him during the course of his employment which is not already in the public domain.[101]

Refusing to mandate judicial review of secrecy classifications, the court did require a judicial determination of whether the information in dispute had in fact been administratively classified. And, though the concession might appear small, it gained significance at the subsequent trial where the district court rejected assertions by CIA officials that all of the 168 disputed passages were classfied and found as a fact that only 27 of the 168 had been.

IMPLICATION OF THE FREEDOM OF INFORMATION ACT

Perceptions of government's economic superiority in the gathering and assembly of facts, data and information in part motivated passage of the Freedom of Information Act to provide "the necessary machinery to assure the availability of government information necessary to an informed electorate."[102] Ironically, it is in this, the most explicit attempt so far to provide a legal mechanism for public access, that the most effective constraint on access to defense-related information appears. Section 552(b)(1) expressly excepts from the Act's coverage matters that are "specifically required by Executive Order to be kept secret in the interest of the national defense or foreign policy," said by the House committee report to embrace those "categories of information which the President has determined must be kept secret to protect the national defense or to advance foreign policy, such as matters classified pursuant to Executive Order 10,501."[103] The exception draws strength not only from the practical burden imposed on information seekers of identifying the information in which they are interested -- essentially the same as is imposed on requests to declassify[104] -- but in the judicial refusal to determine the propriety of any classification.[105]

It seems clear, then, that law is even less effective in securing information from overt, public appropriations, than from those accomplished covertly. The constitutional inhibition on prior restraints

aside, secrecy will in these situations be substantially jeopardized, if not lost altogether, through the processes that typically precede publication in which personnel not subject to security clearance procedures prepare the material for publication. Regulation of the messengers to the press and the public, as through enforcement of secrecy contracts, is only an instance of regulation of covert behavior, and subject to all of its difficulties. Maintenance of secrecy through exception to the Freedom of Information Act, on the other hand, represents not so much an attempt at guarding secrecy as an attempt at not ceding legal access to government-collected data and information. Secrecy, to the extent that it exists, is a product of the government's economic advantage with respect to the information it has assembled, and of the deployment of technical safeguards. As has been seen, however, in the discussions of intelligence procedures, trade secrets and bureaucratic leaks, neither economic nor technical implements have proved particularly effective in maintaining secrecy.

In summary, we began with a proposition that the conventional arguments in favor of closely maintained secrecy: can be reversed under modern conditions without sacrificing the security interests at stake, should be reversed to accommodate official and representative decision-making pressures, and may have to be reversed if the rival will be more effectivly disabled by the dispersion of a mass of undigested information than by the secretion of its more intelligible derivatives.

It should be emphasized that in this report we are concerned solely with the question of secrecy in the common situation where the information hidden can be reconstructed from a larger mass of data, such as that usually encountered in the procurement process. Of course, there are other situations in the world of defense where secrets can and should be maintained. And, even in procurement there are situations where critical information can be concealed and cannot be readily uncovered by mere examination of a larger corpus of data. In these instances secrecy remains a powerful and useful tool.

The basic philosophical tenets underlying the procurement automation system described in Volume I appear not to conflict but, rather, meet the described aims of national security, even though some measure of secrecy may appear necessarily to be abandoned. Of course, no proof is given that the benefits of doing business in a more open manner outweigh the costs in all instances. But, the data suggest that openness is clearly preferable in most instances. And, the detailed program of how such policy might be implemented in Volume I provides a useful proof that increased openness need not entail additional administrative costs.

## FOOTNOTES

1. It should be obvious that this second function is in the United States neither the exclusive preserve of the federal government -- for state and local governments are actively involved in the gathering and management of data -- nor of government generally -- for private firms and the academic establishment contribute, too.

2. If a library holds two copies of the same book, one of them can be destroyed or exchanged without the system's losing information. In the language of Shannon's information theory, multiple copies make the library redundant. But copies are only one of three important forms of redundancy in information. Even if a library has only one copy of each book, it still has a high degree of informational overlap. If half the titles in the Library of Congress were destroyed at random, little of the world's knowledge would disappear.

The most important and subtle form of redundancy derives from the world's being highly lawful. Facts are random if no part of them can be predicted from any other part -- that is, if they are independent of each other. Facts are lawful if certain of them can be predicted from certain others. We need store only the fraction needed to predict the rest.

Simon, *Designing Organizations for an Information-Rich World*, in M. Greenberger, ed., Computers, Communications, and the Public Interest 37, 45 (1971).

3. For one thoughtful examination of the benefits to be conferred by openness in government administration, consider: Oettinger, *Communications in the National Decision-Making Process*, in M. Greenberger, ed., Computers, Communications, and the Public Interest 73 (1971).

4. See supra, p. 5.

5. H. Ransom, The Intelligence Establishment 32 (1970). Dulles himself observed in 1954, "I would give a great deal if I could know as much about the Soviet Union as the Soviet Union can learn about us by merely reading the press...Sometimes I think we go too far in what our government gives out officially and in what is published in the scientific and technical field. We tell Russia too much. Under our system it is hard to control it." Interview with Allen Dulles, U.S. News and World Report 62 (March 19, 1954).

6. Hoover, *The U.S. Businessman Faces the Soviet Spy*, 42 Harv. Bus. Rev. 140, 143 (Jan-Feb 1964).

7. H. Ransom, The Intelligence Establishment 19 (1970).

8. Restatement, Torts, Section 757, comment (b) (1938).

9. Restatement, Torts, Section 757, comment (f) (1938); see, e.g., E.I. Dupont de Nemours & Co. v. Christopher, 431 F.2d 621 (7th Cir. 1971).

10. See, e.g., Forest Laboratories, Inc. v. Formulations Inc., 299 F.Supp. 202 (E.D. Wis. 1969) rev'd in part, 452 F.2d 621 (7th Cir. 1971).

11. See Doyle & Joslyn, *The Role of Counsel in Litigation Involving Technologically Complex Trade Secrets*, 6 B.C. Indust. & Comm. L. Rev. 743, 744 (1965).

12. See, e.g., R. Milgrim, Trade Secrets, Section 1.10 (1974).

13. See, e.g., Forest Laboratories, Inc. v. The Pillsbury Co., 452 F.2d 621 (7th Cir. 1971).

14. See, e.g., Conmar Products Corp. v. Universal Slide Fastener Co., Inc., 172 F.2d 150 (2d Cir. 1949); Schulenburg v. Signatrol, Inc., 33 Ill. 2d 379, 212 N.E.2d 865 (1965); contra, Shellmar Products Co. v. Allen-Qualley Co., 87 F.2d 104 (7th Cir. 1936).

15. See generally, Blake, *Employee Covenants Not to Compete*, 73 Harv. L. Rev. 625 (1960); P. Goldstein, Copyright, Patent, Trademark and Related State Doctrines: Cases and Materials 169-179 (1973).

16. Greene, *Management, Business Intelligence and Espionage*, in R. Greene, ed., Business Intelligence and Espionage 3, 13 (1966).

17. Anon., *An Introduction to Intelligence Systems in Business*, in R. Greene, ed., Business Intelligence and Espionage 41, 49 (1966).

18. Richards, *A Bibliography of Sources for Defense Information*, in R. Greene, ed., Business Intelligence and Espionage 148-165 (1966).

19. Furash, *Industrial Espionage*, 37 Harv. Bus. Rev. 6, 156 (Nov-Dec 1959).

20. To the extent that investment is a function of secrecy, investment need not increase relative to the significance, as measured by market value, of the information involved, for the importance of an innovation is not related to its amenability to secretion. Innovators will, though, be inclined to invest proportionally more to erect safeguards around information they deem valuable, just as competitors will be inclined to invest more in its discovery through espionage, reverse engineering or independent discovery.

21. The Department of Defense has traditionally honored the proprietary nature of information submitted under contract, 32 C.F.R. (1974), a position that is consistent with the behavior of other federal departments and agencies, see generally, Gellhorn, *Business Secrets in Administrative Agency Adjudication*, 22 Admin. L. Rev. 515 (1970).

22. Office of Director of Defense Research and Engineering, Report of the Defense Science Board, Task Force on Secrecy 9 (1970); declassified 1972).

23. See supra.

24. United States v. Russo. No. 9373-(WMB)-DC (filed Dec. 29, 1971), dismissed (C.D. cal. May 11, 1973).

25. P. Schrag, Test of Loyalty 191 (1974). See generally, Nimmer, *National Security Secrets v. Free Speech: The Issues Left Undecided in the Ellsberg Case*, 26 Stan. L. Rev. 311 (1974).

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

27. 403 U.S. 724, 726.

28. Though the point has often been overlooked, attempts at secrecy in this context possess at least two distinct objectives: sequestration of discussion among high government officials and with officials of foreign governments, the revelation of which may serve to chill future such frank and open conversations; and sequestration of information gathered by government, the revelation of which, though it might arguably compromise national security, cannot be expected to lead to diminished intelligence gathering. The first object, though recently the more dramatic focus of public concern, will be considered in this section only by analogy and to the extent that it reveals principles relevant to consideration of the second object.

29. For one, excellent review, see *The National Security Interest and Civil Liberties*, 85 Harv. L. Rev. 1130 (1972).

30. The business of the executive branch is not, of course, the only business of government. Yet, because the executive departments are the primary producers and gatherers of defense-related information, the security information-gathering function of the legislative and judicial branches have focused primarily on wresting this information from the executive grasp.

31. 42 U.S. L. Week 5237 (July 24, 1974).

32. 42 U.S. L. Week 5246.

33. 42 U.S. L. Week 5244.

34. 42 U.S. L. Week 5244.

35. The Court's balancing of interests approach is most clearly expressed at 42 U.S. L. Week 5246 n. 19:

> We are not here concerned with the balance between the President's generalized interest in confidentiality and the need for relevant evidence in civil litigation, nor with that between the confidentiality interest and congressional demands for information, nor with the President's interest in preserving state secrets. We address only the conflict between the President's assertion of a generalized privilege of confidentiality against the constitutional need for relevant evidence to criminal trials.

36. 345 U.S. 1 (1953).

37. 345 U.S. 5 (1953).

38. Upon the government's refusal to produce the requested documents, the district court "entered an order under Rule 37(b)(2)(i), that the facts on the issue of negligence would be taken as established in plaintiff's favor."

39. 345 U.S. 1, 11 (emphasis added).

40. 92 U.S. 105 (1875).

41. 92 U.S. 105, 107.

42. 345 U.S. 11 n. 26.

43. 42 U.S. L. Week 5239

44. 42 U.S. L. Week 5242.

45. See generally, Department of Justice, *Is a Congressional Committee Entitled to Demand and Receive Information and Papers from the President and the Heads of Departments Which They Deem Confidential, in the Public Interest?* in Hearings on S.921 and the Power of the President to Withhold Information from Congress Before the SubComm. on Constitutional Rights of the Sen. Comm. on the Judiciary, 85th Cong., 2d Sess. pt. I at 63, 105 (1958).

46. See *U.S. Government Information Policies and Practices -- The Pentagon Papers*, Hearings Before a Subcom. of the House Comm. on Gov't Operations, 92d Cong., 1st Sess., pt. 2 at 682 (statement of David Cooke).

47. Congressmen may not even know what questions to ask in attempting to probe the Government's conduct. The experience of the Senate Foreign Relations Committee in attempting to find out the extent of American military involvement in Laos illustrates this problem. In a 1969 hearing before the Committee, the American Ambassador to Laos testified that the United States had no military training or advisory units in Laos and that Air America operations were limited solely to transporting equipment for programs under the Agency for International Development. The Ambassador neglected to mention the large-scale bombing missions being conducted by the U.S. Air Force. At later hearings, after the existence of bombing missions became declassified information, the Ambassador was asked about this omission. He explained that he had not been asked any questions about operations in northern Laos. Senator Fulbright commented: 'We do not know enough to ask you these questions unless you are willing to volunteer the information. There is no way for us to ask you questions about things we don't know you are doing.'
*The National Security Interest and Civil Liberties*, 85 Harv. L. Rev. 1130, 1210 (1972).

48. 32 C.F.R. Section 155.4(a) (1974).

49. 32 C.F.R. Section 155.5(a), (e), (m) (1974).

50. See Foreign Affairs Division, Legislative Reference Service, Library of Congress, 92d Cong., 1st Sess., Security Classification as a Problem in the Congressional Role in Foreign Policy 3 (Comm. Pring 1970).

51. Act of July 27, 1789, ch. 4 Section 4, 1 Stat. 28.

52. R.S. Section 161 (1875).

53. 16 Fed. Reg. 9795 (1951).

54. 3 C.F.R. 979 (1949-53 Comp.).

55. See, e.g., Exec. Order 10, 964, 3 C.F.R. 159-63 Comp. 486 (1964).

56. 3 C.F.R. 375 (1973).

57. C. Barker & M. Fox, Classified Files: The Yellowing Pages, p. 12 (1972).

58. *U.S. Government Information Policies and Practices -- The Pentagon Papers*, Hearings Before a Subcomm. of the House Comm. on Government Operations, 92d Cong., 1st Sess. pt. I, at 97 (statement of William Florence).

59. The Nixon Order, its antecedents and implications, are considered in *Reform in the Classification and Declassification of National Security Information: Nixon Executive Order 11652*, 59 Iowa L. Rev. 110 (1973).

60. 3 C.F.R. 380 (1973).

61. 3 C.F.R. at 380-81.

62. 3 C.F.R. 382.

63. 3 C.F.R. 381.

64. *National Security Council Directive Governing the Classification, Downgrading, Declassification and Safeguarding of National Security Information*, 37 Fed. Reg. 10, 053, 10067 (1972); 3 C.F.R. 384.

65. *National Security Council Directive Governing the Classification, Downgrading, Declassification and Safeguarding of National Security Information*, 37 Fed. Reg. 10, 053, 10056 (1972); 3 C.F.R. 383-84.

66. *National Security Council Directive Governing the Classification, Downgrading, Declassification and Safeguarding of National Security Information*, 37 Fed. Reg. 10, 053, 10, 061-62 (1972).

67. 3 C.F.R. 382.

68. 3 C.F.R. 375, 381. See generally, *Reform in the Classification and Declassification of National Security Information: Nixon Executive Order 11652*, 59 Iowa L. Rev. 110, 124-125 (1973).

69. See generally, *The National Security Interest and Civil Liberties*, 85 Harv. L. Rev. 1130, 1205-06 (1972).

70. Frankel, *The "State Secrets" Myth*, Columbia Journalism Review 22 (Sep-Oct 1971).

71. See generally, M. Halperin, Bureaucratic Politics and Foreign Policy 173-195 (1974). The Halperin study draws extensively upon incidents and observations recorded in the published memoirs of officials who have served in the national security bureaucracy since World War II, and several of these recollections, together with Halperin's analysis, form the main foundation for this section of the paper.

72. See, for example, incidents recounted at M. Halperin, Bureaucratic Politics and Foreign Policy 180-181 (1974).

73. Leaks to the press can be designed to affect relations between organizations as well as individuals when this is believed necessary in order to attain a desired outcome. The Army, attempting to get permission for

development of medium-range missile, at one point sought to cement an alliance with the Navy by inflaming relations between the Navy and the Air Force. Army colonels leaked to the Pentagon reporter of the *New York Times* an Air Force staff paper which deprecated the contribution of Forrestal-class carriers to the overall strategic mission. The aim was to deceive the Navy into thinking that the Air Force was leaking papers prejudicial to the Navy's interest.

M. Halperin, Bureaucratic Politics and Foreign Policy 179 (1974).

74. See examples cited at M. Halperin, Bureaucratic Politics and Foreign Policy 177-179 (1974).

75. Compare R. Hilsman, To Move a Nation: The Politics of Foreign Policy in the Administration of John F. Kennedy 499 (1967).

76. See F. Rourke, Secrecy and Publicity 23 (1961).

77. C. Barker & M. Fox, Classified Files: The Yellowing Pages, App. 3, pp. 106, 108 (1972).

78. The main espionage statutes are codified as 18 U.S.C. 793-798 (1970).

79. The two sections do, however, discriminate in terms of the penalties prescribed.

80. United States v. Russo, No. 9373-(WMB)-CD (filed Dec. 29, 1971), dismissed (C.D. Cal. May 11, 1973).

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

82. See generally, Edgar & Schmidt, *The Espionage Statutes and Publication of Defense Information*, 73 Colum. L. Rev. 929, 972-974 (1973).

One proposed resolution of this definitional difficulty would identify information related to the national defense with information that has been administratively classified. This approach has in fact been taken in 50 U.S.C. Section 783 (b), which prohibits federal employees from communicating to foreign agents "any information of a kind which shall have been classified by the President ...as affecting the security of the United States."

The benefits -- precision and efficiency in management of the judicial resource -- presumably offered by use of administrative classification to definitional ends, seem largely illusory. As has already been shown, the few constraints on the classification process hardly guarantee that subject matter classified has any bearing on the national defense, even broadly conceived. This suggests that questions of the procedural and substantive propriety of the classification in issue would probably become the subject of judicial review, with only some presumption of validity accorded

the administrative decision. Finally, the approach lends no guidance to policy in the most problematic area -- where the classified information can be reconstructed from facts and data available in the public domain.

83. 151 F.2d 813 (2d Cir. 1945) cert. denied, 328 U.S.C. 833 (1946).

84. 151 F.2d 813, 815.

85. 151 F.2d 813, 816.

86. 312 U.S. 19 (1941).

87. 312 U.S. 27-28.

88. 312 U.S. 28.

89. Edgar & Schmidt, *The Espionage Statutes and Publication of Defense Information*, 73 Colum. L. Rev. 929 (1973).

90. 403 U.S. 713 (1971).

91. 403 U.S. 713, 724 (Brennan, J. concurring).

92. 403 U.S. 713, 740 (Marshall, J. concurring).

93. 403 U.S. 713, 714, 720 (Black and Douglas, J. J., concurring).

94. 403 U.S. 713, 750.

95. Henkin, *The Right to Know and the Duty to Withhold: The Case of the Pentagon Papers*, 120 U. Pa. L. Rev. 271, 277 (1971).

96. See supra, pp. 12-18.

97. United States v. Marchetti, 466 F.2d 1309 (4th Cir.), cert. denied, 93 S. Ct. 553 (1972).

98. 5 U.S.C. Section 552 (as amended Supp. V 1970).

99. 466 F.2d 1309, 1311.

100. 466 F.2d, 1309, 1313.

101. 466 F.2d, 1309, 1317 (emphasis added).

102. H.R. Rep. No. 1497, 89th Cong. 2d Sess. 12 (1966).

103. H.R. Rep. No. 1497, 89th Cong. 2d Sess. 9-10 (1966).

104. See supra, pp. 29-31.

105. See, e.g., Environmental Protection Agency v. Mink, 410 U.S. 73 (1973).