Union Calendar No. 908

96th Congress, 2d Session - - - - - - - House Report No. 96-1540

THE GOVERNMENT'S CLASSIFICATION OF PRIVATE IDEAS

THIRTY-FOURTH REPORT

BY THE

COMMITTEE ON GOVERNMENT OPERATIONS

together with

ADDITIONAL VIEWS

DECEMBER 22, 1980.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

---

U.S. GOVERNMENT PRINTING OFFICE

WASHINGTON : 1980

82-089 O—82——1 (Pt. 5) BLR

COMMITTEE ON GOVERNMENT OPERATIONS

JACK BROOKS, Texas, *Chairman*

L. H. FOUNTAIN, North Carolina
DANTE B. FASCELL, Florida
WILLIAM S. MOORHEAD, Pennsylvania
BENJAMIN S. ROSENTHAL, New York
FERNAND J. ST GERMAIN, Rhode Island
DON FUQUA, Florida
JOHN CONYERS, JR., Michigan
CARDISS COLLINS, Illinois
JOHN L .BURTON, California
RICHARDSON PREYER, North Carolina
ROBERT F. DRINAN, Massachusetts
GLENN ENGLISH, Oklahoma
ELLIOTT H. LEVITAS, Georgia
DAVID W. EVANS, Indiana
TOBY MOFFETT, Connecticut
ANDREW MAGUIRE, New Jersey
LES ASPIN, Wisconsin
HENRY A. WAXMAN, California
FLOYD J. FITHIAN, Indiana
PETER H. KOSTMAYER, Pennsylvania
TED WEISS, New York
MIKE SYNAR, Oklahoma
ROBERT T. MATSUI, California
EUGENE V. ATKINSON, Pennsylvania

FRANK HORTON, New York
JOHN N. ERLENBORN, Illinois
JOHN W. WYDLER, New York
CLARENCE J. BROWN, Ohio
PAUL N. McCLOSKEY, JR., California
THOMAS N. KINDNESS, Ohio
ROBERT S. WALKER, Pennsylvania
ARLAN STANGELAND, Minnesota
M. CALDWELL BUTLER, Virginia
LYLE WILLIAMS, Ohio
JIM JEFFRIES, Kansas
OLYMPIA J. SNOWE, Maine
WAYNE GRISHAM, California
JOEL DECKARD, Indiana

WILLIAM M. JONES, *General Counsel*
JOHN E. MOORE, *Staff Administrator*
ELMER W. HENDERSON, *Senior Counsel*
JOHN M. DUNCAN, *Minority Staff Director*

GOVERNMENT INFORMATION AND INDIVIDUAL RIGHTS SUBCOMMITTEE:

RICHARDSON PREYER, North Carolina, *Chairman*

ROBERT F. DRINAN, Massachusetts
GLENN ENGLISH, Oklahoma
DAVID W. EVANS, Indiana
PETER H. KOSTMAYER, Pennsylvania
TED WEISS, New York

THOMAS N. KINDNESS, Ohio
M. CALDWELL BUTLER, Virginia
JOHN N. ERLENBORN, Illinois

EX OFFICIO

JACK BROOKS, Texas
FRANK HORTON, New York

TIMOTHY H. INGRAM, *Staff Director*
GERALD R. STURGES, *Professional Staff Member*
THOMAS G. MORR, *Minority Professional Staff*

LETTER OF TRANSMITTAL

HOUSE OF REPRESENTATIVES,
Washington, D.C., December 22, 1980.

Hon. THOMAS P. O'NEILL, Jr.
Speaker of the House of Representatives,
Washington, D.C.

DEAR MR. SPEAKER: By direction of the Committee on Government Operations, I submit herewith the committee's thirty-fourth report to the 96th Congress. The committee's report is based on a study made by its Government Information and Individual Rights Subcommittee.

JACK BROOKS, *Chairman.*

CONTENTS

96TH CONGRESS } HOUSE OF REPRESENTATIVES { REPORT
2d Session } { No. 96–1540

THE GOVERNMENT'S CLASSIFICATION OF PRIVATE IDEAS

DECEMBER 22, 1980.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. BROOKS, from the Committee on Government Operations, submitted the following

THIRTY-FOURTH REPORT

together with

ADDITIONAL VIEWS

BASED ON A STUDY BY THE GOVERNMENT INFORMATION AND INDIVIDUAL RIGHTS SUBCOMMITTEE

On December 2, 1980, the Committee on Government Operations approved and adopted a report entitled "The Government's Classification of Private Ideas." The chairman was directed to transmit a copy to the Speaker of the House.

I. INVENTION SECRECY

A. GENERAL STATEMENT OF FINDINGS

The invention secrecy enterprise was founded and shaped in times of war. Its patterns of practice were woven in World War II. It functions today without peacetime philosophy or scrutiny. It conflicts with the principles of the patent system.

Congress explored invention secrecy issues in 1950, before the Korean conflict, and in 1951, but did not resolve the main ones. After President Truman's proclamation of emergency in December 1950, Congress was disposed to grant the repeated request of the Defense Department for renewed invention secrecy authority. It wrote the Invention Secrecy Act of 1951 and included a bridging provision which allowed secrecy orders to become semipermanent.

Secrecy orders then in effect or issued during the national emergency could remain in effect without review or reconsideration for the duration of the emergency plus six months. As it happens, this stopgap served for 27 years, until March 1979. The number of secrecy

orders rose from 3,435 in midsummer 1951 to 6,149 at the end of 1958, then fluctuated between 4,100 and 5,100 for the next 20 years. Congress should now confront the issues it postponed in 1951.

The Patent and Trademark Office waits table for invention secrecy. It must bring a secrecy order when beckoned by a Government agency and cannot remove the order until told to do so. It can do little more than try to dissuade the agency from requesting an order on grounds that the invention involved has already been published. When it receives a patent application bearing security classification markings, it attempts to verify the authority of the classifier but not the propriety of the classification.

For 40 years the Armed Services Patent Advisory Board has served as principal but not sole agent of the defense agencies for invention secrecy matters and requested over 41,000 secrecy orders. If the Navy, say, wishes a secrecy order on its own patent application, it deals directly with the Patent Office. Technical review of patent applications to determine whether they should be placed under secrecy is performed not by ASPAB but by personnel of the separate uniformed services.

The invention secrecy enterprise tends itself, like an automated lighthouse. The basis for issuance of a secrecy order is the opinion of an agency head that disclosure "would be detrimental to the national security"—less demonstrable than the "which reasonably could be expected to cause . . . damage to the national security" standard incorporated in the current executive order for classifying national security information. How an agency heads forms such an opinion is not subject to higher review or Patent Office challenge. His opinion is final until he changes it, yet in the defense agencies his authority to form such an opinion has been delegated and redelegated into the ranks.

There is no mention of invention secrecy in the mandatory annual report of the Commissioner of Patents and Trademarks to Congress. Neither ASPAB nor the Patent Office keeps track of compensation paid to inventors for damages resulting from secrecy orders. Agencies can record their interests in patents and patent applications in a secret register at the Patent Office. Invention secrecy transactions are shielded by Patent Office confidentiality, classified agency documents and, in some cases, gaps in public files.

No secrecy order ever underwent judicial review for appropriateness. There has been no First Amendment judicial test of the Invention Secrecy Act, and the statutory right of an inventor to just compensation for secrecy order damages appears more illusory than real.

B. Findings

1. Invention secrecy as currently constituted is heavily weighted against private inventors who work outside the classified and defense community. Invention secrecy undergirds and aggrandizes the military-industrial complex, and ensnares the inventors who work outside of the classified information community. It gives these nonmember inventors the choice of presenting their discoveries to the public without ownership protection, or of trying to obtain a patent and thereby risking Government confiscation of their ideas. In the shoptalk of the

Armed Services Patent Advisory Board, these nonmember inventors are characterized collectively as "John Does."

2. Congress never set down a rationale for invention secrecy in peacetime. It avoided that issue in legislating the Invention Secrecy Act of 1951 by granting secrecy orders a lifetime six months beyond the duration of President Truman's December 1950 proclamation of national emergency. The Truman proclamation shielded these orders for 27 years, until March 1979.

3. From its inception in 1917, invention secrecy was premised on the fact or imminent prospect of war. The Invention Secrecy Act of 1951 extended it in the expectation of a formal end to World War II hostilities, which would have unveiled existing secrecy orders, and the Korean conflict, which implied a need for new ones. Now, invention secrecy thrives on the presumption that war is not merely possible, but likely. This creates the anomaly that invention secrecy authority has been limited in time of war, but is now assumed to be permanent in time of peace.

4. The basis for issuance of a secrecy order—the opinion of an agency head that disclosure "would be detrimental to the national security"—is subjective and absolute. It is one of more than 240 references in the United States Code (1970) to national security as a policy condition: "for reasons of * * *," "for purposes of * * *," "in the interest of * * *," "detrimental to * * *." On this broad standard, what might be deemed detrimental can vary widely with the times and the agency.

Consider paint. During World War II, naval vessels used a copper-based paint, developed by the Navy at its Mare Island, Calif., facility and designated HP–15, which permitted them to stay at sea for 18 months with practically no loss of speed, where before they had to go to dock every six months or so. Navy patent counsel testified in 1950 he could give anyone a barrel of that paint and defy his analyzing and making it "within any reasonable time," but that a patent application for the paint would deserve a secrecy order because it "is a book which tells the complete story." Years later, the Navy developed an organo-metallic-polymer (OMP) antifouling paint and decided to exploit it commercially. A promotional handbill in the National Technical Information Service "Selected Technology for Licensing" series advertised that one application of this antifouling compound can keep ship hulls and other submerged objects barnacle-free for up to five years. The Navy now has three patents on OMP-type compounds, none of which was ever subjected to secrecy order, and 24 licensees.

5. The Invention Secrecy Act has been overtaken by the national security information system. The act makes no reference to this system, then defined by President Truman's Executive Order 10290 of September 24, 1951, but invention secrecy practitioners regard it as necessary and sufficient for a Government or contractor patent application to contain classified information to qualify for a statutory secrecy order. In July 1980, for example, the Armed Services Patent Advisory Board was considering sending a letter to the Information Security Oversight Office which described the statutory invention secrecy scheme in these terms: "a secrecy order is imposed upon the classified patent application at the request of a defense agency"; "This secrecy order is renewed annually and remains in effect while *any portion* of the application is classified" (emphasis in original); "After the ap-

plication becomes unclassified, the defense agency requests rescission of the secrecy order, and the Patent and Trademark Office is notified that the security markings can be removed from the entire document. Then the patent issues."

In this view, imposition of a secrecy order flows from the judgment of some member of the classified community that the patent application contains, cites or would compromise classified information. Here is an example from subcommittee files of the connection between a secrecy order and a military widget whose very material was classified:

In November 1963, a secrecy order was imposed on a Conductron Corporation patent application for radar-absorbing ferrite tiles. Conductron, of Ann Arbor, Mich., manufactured these magnetic absorbers for use in the F–111 aircraft. The tiles themselves were classified "Confidential," apparently because laboratory analysis of them could have revealed radar attenuation and response. "For reasons of security, safety, and furnace contamination problems," Conductron noted, "the process of destroying the material is formidable as well as expensive." By June 1970, Conductron had 27,000 pounds of classified scrap ferrite material on hand awaiting destruction. The Air Force, acknowledging that the material could be destroyed only by incineration in a high-temperature blast furnace in the presence of reduced atmosphere, was faced with expenditures of around $650,000 to dispose of the waste titles that had accumulated at various locations. (Since the molten metal retained some of the electrical properties that caused it to be classified in the first place and would have stuck to the furnace walls, the furnace would have become classified "Confidential.")

Given these factors, "and the period of time which has elapsed since the initial classification decision and the current state of the art," the Air Force declassified the titles in September 1970. However, the secrecy order on the patent application remained in effect until February 1975. In February 1976, a patent on the magnetic absorbers was issued to Dale M. Grimes and three other inventors (and assigned to McDonnell Douglas Corp., which had since acquired Conductron).

For all its reliance upon the national security information system, the classified community has yet to demonstrate to the committee that a secrecy order cannot be imposed on a Government or contractor patent application until and unless it fulfills executive order requirements for the classification of documents. Further, nonmember inventor applications, the ones filed by "John Does," apparently can be classified before undergoing secrecy order, since paragraph 1–603 of President Carter's Executive Order 12065 on national security information ("A product of non-government research and development that does not incorporate or reveal classified information to which the producer or developer was given prior access may not be classified under this Order until and unless the government acquires a proprietary interest in the product.") expressly does not affect the provision of the Invention Secrecy Act.

The Armed Services Patent Advisory Board manual provides, "Patent applications under secrecy order require treatment as security classified information until a rescind order has actually issued." It further provides that whether or not patent applications being circulated bear military security classification markings, they should be

treated as if they contained information classified at not less than "Confidential."

5a. Within the classified community, invention is regarded as the mother of necessity. Yet there appears to be no comparable belief in the necessity of maintaining classification practices and procedures to contemporary standards. For example, the August hearing disclosed that the ASPAB field-of-interest list on file at the Patent Office—which guides it in selecting patent applications for technical review by defense agencies—was classified in 1971 and has not been classified in accordance with President Carter's EO 12065 issued in June 1978. The August hearing also dealt with a Patent Office form called a Markings Letter, which "requests applicant to determine need for existing classification markings in case." It is sent after rescission of a secrecy order if the Patent Office finds that the patent application file contains classified information. This form (PTOL–248), last revised in March 1978, begins:

> Papers in the file of this application bear thereon security classification markings under Executive Order 10,501, dated October 15, 1953.

That order by President Eisenhower was revoked and superseded in 1972 by President Nixon's Executive Order 11652. Defense Department witnesses could not explain why the Patent Office form is anchored in an outdated executive order. The form then misstates the law by alleging:

> Such markings preclude normal prosecution of applications and would, of course, make it a violation of the Espionage Act to publish, or for an applicant to permit publishing of, the classified subject matter as for example by the grant of a patent or by appeal to a court.

The Markings Letter illustrates how a form used to implement a lawful activity can contain archaic and spurious information.

6. The Patent and Trademark Office and defense agencies have misapplied the Invention Secrecy Act by blurring the distinction it makes between the Government's having or not having a property interest in a patent application. The unambiguous distinction is that when an agency has a property interest, it and it alone is entitled to request a secrecy order. When no agency holds a property interest in an application, the Patent Office refers it to the defense agencies likely to want a secrecy order, and one of them decides whether to request an order.

Circulating to other agencies a patent application in which, say, the National Science Foundation holds an interest, flies in the face of the plain meaning of the act and the clear statement of intent in the accompanying House report. Perhaps this unauthorized practice took hold as the NSF and other nondefense agencies developed larger funding roles over the years in basic research, so that more and more inventions resulting from these grants and contracts were placed outside of the defense perimeter.

The following table supplied by the National Science Foundation illustrates the change in level and sources of Federal support for basic research that occurred between 1952 and 1980:

FEDERAL OBLIGATIONS FOR BASIC RESEARCH, BY SELECTED DEPARTMENTS AND AGENCIES

[In millions of dollars]

Agency	Fiscal year— 1952	1980, estimate
Total	162	4,512
Department of Health and Human Services [1]	15	1,716
National Institutes of Health	(14)	(1,592)
National Science Foundation	1	814
National Aeronautics and Space Administration [2]	18	535
Department of Energy [3]	34	523
Department of Defense	72	429
Department of Agriculture	7	288
Department of the Interior	8	75
All others	7	132

[1] Federal Security Agency in 1952.
[2] National Advisory Committee for Aeronautics in 1952.
[3] Atomic Energy Commission in 1952.

Sources: National Science Foundation for 1952 data; Office of Management and Budget for 1980 data with 1980 expected revisions as of Apr. 14 1980.

The Armed Services Patent Advisory Board itself acknowledged this distinction in 1953 in discussing its proposed charter. When the charter originally submitted was questioned on grounds that the Invention Secrecy Act vested authority in the Secretary of Defense, it was agreed that the secretaries of the military departments do have some authority vested in them "where the military departments have a property interest in an invention * * *" (see note 98 and accompanying text in the historical section of this report). It should be obvious that the defense agencies are not free to insist upon the property interest distinction with respect to their own patent applications and ignore it as it applies to other agencies.

7. The hallways of invention secrecy are cluttered with bureaucratic bric-a-brac: special handling, special access, the five-year rule, the immediate action letter, the joint signoff on secrecy order rescission, and so on. Most are of World War II origin, and some—or perhaps most—have been removed. These administrative shortcuts and techniques lack statutory foundation. They serve the convenience of the Patent Office and the defense agencies, but it has not been shown that they serve the national interest. Congress clearly believed in 1951 that invention secrecy in peacetime was drastic business. The committee agrees, and recommends that these workaday adornments be removed.

8. The right to administrative compensation set forth in the Invention Secrecy Act is more illusory than real. The subcommittee received testimony that 29 administrative claims for compensation have been filed with the Defense Department since 1945, before the act was passed. Of these, five are the subjects of pending litigation, three were settled by the Defense Department before litigation, five were settled during litigation, one was the subject of a private relief bill, 10 were terminated by denial, and the remainder are pending, according to the testimony.

That approximates one claim for every thousand secrecy orders requested by the Armed Services Patent Advisory Board. The disposition of the 29 claims indicates that few are settled promptly and satisfactorily, without litigation in U.S. District Court or the Court of

Claims. Some settlements involve significant sums, but the Army Judge Advocate General's office points out that invention secrecy claims generally are encompassed within a much more substantial claim for infringement of a subsequent patent, and secrecy order damages frequently reflect a small part of the total settlement.

Under earlier statutes, a secrecy order recipient was entitled to compensation only if the Government used the invention. To qualify, one first had to offer an invention to the Government for its use, then wait until a patent issued. The Invention Secrecy Act removed these limitations, declaring that an applicant under secrecy order has the right to seek just compensation from the agency that caused the order to be issued: damage caused by the order itself and/or for the use of the invention by the Government. And one can apply for compensation as soon as the Patent Office determines an invention is patentable.

Congress undoubtedly eased the terms of compensation in exchange for continuing the invention secrecy enterprise in peacetime. The results have been disappointing. Agencies can specify the form and content of an administrative claim, and may attempt to require by regulation nearly as much supporting evidence for the claim as they could expect to collect by rule of discovery in a court of law. Agencies have little or no incentive to settle a claim. The claimant frustrated by agency delays can drop the matter or bring suit and then deal with Justice Department attorneys.

Defense agencies take the position that the applicant suffers no damages from a secrecy order when the invention was intended exclusively for a Government market and the Government does not use the invention. In this view, any claim of damages is wholly speculative, since the applicant has no market by which to substantiate the claimed value of an invention. The secrecy order is deemed incapable of inflicting damages in and of itself.

Of course, a Government contractor under secrecy order may make and sell an invention to the Government, and even be permitted to sell the product or process overseas, suffering no damages except to the extent the secrecy order deprives it of other Government or commercial markets. For example, in the radar-absorbing ferrite tile case mentioned above, the manufacturer, Conductron Corporation, informed the Air Force in June 1970 there were "certain commercial applications, mostly relating to anechoic chambers and antenna design, for which these ferrites would be ideal," as well as "numerous military applications where this material can be used in small quantities," but that it was prevented from informing "most of the engineering personnel within the Government and industry that such a material exists." The Air Force declassified the tiles in September 1970 in part because of "the current state of the art" in electromagnetic absorption but the secrecy order on the ferrite tiles patent application stood until February 1975.

Two of the largest settlements are instructive:

(1) In 1961, the military departments settled an administrative claim filed by International Telephone and Telegraph for use of a radar invention. The invention was disclosed in a patent application which was under secrecy order from 1941 to 1945 and which finally issued as a patent in 1957. The claim asserted use resulting from disclosure incidental

to the invention secrecy process, infringement of the patent, and use of the patent in foreign assistance programs. Settlement involved payment of $1 million for all past claims and a future license for an annual ceiling of $300,000 for five years, reduced to $200,000 for the following seven years.

(2) In 1977, litigation by the General Electric Company was settled by the Government. The case involved the Government's use of a radar invention. The patent application was under secrecy order from 1941 to 1945, and the Government's use of the invention had been licensed in part. The claim for use during the period of the secrecy order, for use of the invention incidental to foreign assistance activities, and for infringement of patent which issued in 1958 was settled by payment of $400,000. By concurrent license agreement, the Government purchased a paid-up license for future use of the patent invention for $875,000.

These examples suggest that claimants who are financially strong enough and persistent enough can collect eventually. The Fifth Amendment question posed by the Invention Secrecy Act is whether the Government was granted eminent domain or police powers over all the ideas within its jurisdiction, and whether patent applicants truly receive just compensation for the taking. These issues are central to peacetime invention secrecy and must be resolved.

9. Whether a nonexclusive right acquired by the Government under contract constitutes a property interest for invention secrecy purposes remains unclear 29 years after the question was raised by Roland C. Anderson, Chief of the Patent Branch, Atomic Energy Commission. At the 1951 hearings, Anderson asked:

> Does that mean if the Government merely acquires an interest, a nonexclusive right under its contract, that that is called a property interest? That was the kind of thing we tried to find out, what is the intention; whether it was necessary to have complete title, or anything less than complete title, which might be called a nonexclusive right, which sometimes has been the case of Government-owned property, and whether that would be an interest that would be intended here.

Anderson was told that would be explained in the committee report, but it was not. The House report, which also became the Senate report, simply said that the phrase "property interest"

> is intended to include the ownership of all rights in the invention or to a lesser interest therein such as, for example, cases where the foreign rights are retained by the inventor, or where the Government is entitled only to the interest of one or more joint inventors, and not to the interest of all the joint inventors.

The question evidently has not been judicially tested. For example, in its opinion in *Ocean Science & Engineering, Inc.*, v. *United States*, in which plaintiffs alleged Government infringement of a patent by using the claimed invention on the Glomar Explorer, the U.S. Court of Claims declared:

> Since our ruling on the subject of infringement allows us to refrain from determining whether the government has such a right to a license under these circumstances, we omit Trial Judge Browne's discussion of the issue, and reserve for another time consideration of the scope of patent rights clauses commonly found in government research grants. 595 F.2d 572, 574 (Ct. Cl. 1979) (per curiam).

In the national security information context, the Government now uses the phrase "proprietary interest." President Carter's Executive Order 12065 provides that privately generated information "may not be classified under this Order until and unless the government acquires a proprietary interest in the product." Ironically, the phrase "property interest" is juxtaposed by reference, in that the next sentence of the order stipulates that its provisions do not affect the Invention Secrecy Act.

The phrase "proprietary interest" conveys a sense of something less than complete title. To use the phrase in free substitution for the statutory wording begs the question as yet unanswered by Congress or the courts. How easily the Government can assert an interest determines how readily private ideas can be forced into the national security information system or into the statutory scheme of invention secrecy.

10. Regulations of the Patent and Trademark Office implementing invention secrecy raise serious questions of due process. First, they require an applicant contesting a secrecy order to protest it to the sponsoring agency before pursuing his statutory right of appeal to the Secretary of Commerce. The regulations thus adopt a provision of the invention secrecy bill as introduced in the House in July 1951 but deleted from it in the amended committee print of August 21—the same revision that added the presidentially declared national emergency provision. The Patent Office viewpoint—testimony that "(i)t certainly is in the best interests of national defense and the applicant himself to have an appeal heard and decided at the lowest qualified administrative level"—subordinates the applicant's guarantee of due process to the wishes of the classified community.

Second, the regulations hold, and testimony confirmed, that a secrecy order applies to the subject matter of a patent application even if the application is abandoned. This regulatory posture might not be troublesome if it were confined to technically abandoned applications in which the claims, description or references engendering the secrecy order are carried forward in a continuation-in-part application. In this situation, the invention is not abandoned, even though the application is.

What the Patent Office appears to insist is that the secrecy order applies until it is revoked, regardless of the condition of the applicant's intellectual property vehicle. The Patent Office is arguing that the secrecy order attaches to the nub of something that remains when the patent vehicle is gone. (The defense agencies argue the opposite when the context is compensation, i.e. that nothing inheres—at least nothing of recognizable value—until patentability has been ascertained.) The practitioners of invention secrecy cannot have it both ways.

11. The number of secrecy orders in force today appears to be the lowest since the summer of 1951. This is also the first full calendar year in the history of invention secrecy in which secrecy orders have not enjoyed longer life by virtue of a state of war or of national emergency. It remains to be seen whether defense agencies and the Patent Office can administer invention secrecy on a strictly annual basis.

Secrecy orders now lapse after one year unless there is an affirmative determination that they should be renewed for a year. Technical personnel must now review some 3,500 secrecy orders per year for renewal purposes, as well as upwards of 4,000 new patent applications per year—depending on the number of discretionary referrals by the Patent Office—as potential candidates for a secrecy order. It is entirely possible that the economy and efficiency of the secrecy enterprise will suffer, that the Secret Group in the Patent and Trademark Office (a patent office unto itself) will be overburdened, or that secrecy orders will become either to hard or too easy to obtain.

In June 1979, the Patent Office instituted a new processing step in the initial handling of applications, before their screening for security purposes. Because of inadequate staff to perform this and other necessary processing steps, the inventory of applications destined for security screening rose from 17,300 (representing about 41 work days of processing time) at the end of June, to about 27,000 applications (equalling a processing time of 64 work days) as of mid-January 1980. The new processing step was then suspended, and by the end of March the inventory had been reduced to 18,000 applications representing 42 work days.

The longer it takes an application to wend its way to secrecy screening, the less time defense agencies have to review it before the six-month mark is reached and the applicant by law, has an implied license to file overseas (although applicants tend to wait until the eleventh month before doing so).

12. Defense Department authority for the everyday conduct of invention secrecy has been delegated and redelegated far down into the military and civilian ranks. When the subcommittee chairman commented on the absence of a representative of the Secretary of Defense at the August hearing, the chairman of the Armed Services Patent Advisory Board responded:

> Mr. Chairman, with respect to your regrets regarding someone from the Office of the Secretary of Defense being here, the responsibility for administering and processing matters under the Invention Secrecy Act have been delegated down through the Secretaries of the Services and to this board, and in past history, if you will look at what has happened during the late 40's and early 50's, witnesses before congressional subcommittees and committees were approximately at the level of the personnel here.[1]

The witness' statement about past practice was correct, but the committee notes that those appearances occurred before the Invention Secrecy Act of 1951 vested principal authority for invention secrecy in the Secretary of Defense. The committee believes it is entitled to as-

[1] Testimony in hearings.

sume from the absence of a representative of the Secretary at the August hearing—despite the subcommittee's explicit request that the Pentagon witness team be headed by one—that no one in the Office of the Secretary of Defense is sufficiently knowledgeable about the statute and its implementation to appear in a congressional fact-finding forum. It follows that the committee's concern about the long-distance delegation of the Secretary's authority is confirmed.

13. The Invention Secrecy Act allows patent applications to be sealed by the Commissioner of Patents and Trademarks upon a "proper showing" by an agency head that disclosure would "jeopardize" national security. Defense Department witnesses, however, were unable to explain what constitutes a "proper showing." They testified:

> That would depend on the specific situation. It would presumably involve a written communication from an appropriate official in an agency asking that the patent application be sealed.[2]

Nor would they say or surmise how the Commissioner evaluates the showing as "proper" ("We have no information and defer to the Commissioner on this question." [3]).

DOD rarely uses this authority and has two cases currently under seal. These are considered so sensitive that not even security-cleared patent examiners are allowed to see them. Generally, according to the testimony, only two persons see such applications: the one who places it in a sealed envelope and the one who has requested that it be sealed. The ASPAB chairman said the renewal of the secrecy order on a sealed application is automatic and unreviewed.

Testimony established that the two sealed applications are Air Force cases, that one is a British origin case and that the other—an Air Force contractor development—was ordered under seal by William J. Perry, Under Secretary of Defense for Research and Engineering.

C. Discussion

Introduction

Eminent domain is the right or power of a government to take private property for public use. The eminent domain principle is most often discussed in relation to the taking of real property, but it applies as well to intangible property (". . . patent rights, franchises, charters or any other form of contract, are within the scope of this sovereign authority as fully as land or other tangible property." [4]) In discussing compensation in patent situations, the United States Supreme Court long ago stated:

> That the government of the United States when it grants letters-patent for a new invention or discovery in the arts, confers upon the patentee an exclusive property in the patented invention which cannot be appropriated or used by the government itself, without just compensation, any more than it can appropriate or use without compensation land which

[2] Id., Richard S. Sciascia.
[3] Id.
[4] Julius Sackman, "Nichols' The Law of Eminent Domain" Sec. 2.1(2), (rev. 3d ed. 1976).

> has been patented to a private purchaser, we have no doubt. The Constitution gives to Congress power "to promote the progress of science and useful arts by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries," which could not be effected if the government had a reserved right to publish such writings or to use such inventions without the consent of the owner. Many inventions relate to subjects which can only be properly used by the government, such as explosive shells, rams, and submarine batteries to be attached to armed vessels. If it could use such inventions without compensation, the inventors could get no return at all for their discoveries and experiments. It has been the general practice, when inventions have been made which are desirable for government use, either for the government to purchase them from the inventors, and use them as secrets of the proper department; or, if a patent is granted, to pay the patentee a fair compensation for their use.[5]

Webster's New Collegiate Dictionary (1977) explains the right of eminent domain exists "by virtue of the superior dominion of the sovereign power over all lands within its jurisdiction." The subcommittee's inquiry concerns the extent of the Government's parallel authority over ideas.

A. BACKGROUND

A patent is a 17-year right of exclusive use given the inventor in exchange for his disclosure of the invention so that it will be available for free public use when the patent period expires. By law, all the information in a patent application is held in confidence by the Patent and Trademark Office until the patent actually issues, although nothing prevents an applicant from disclosing his invention to the public before the patent is granted.

In 1917, however, Congress provided that "whenever during a time when the United States is at war the publication of an invention by the granting of a patent might, in the opinion of the Commissioner of Patents, be detrimental to the public safety or defense or might assist the enemy or endanger the successful prosecution of the war he may order that the invention be kept secret and withhold the grant of a patent until the termination of the war." [6] Congress broadened this authority in 1940 by deleting the requirement that the United States be at war and by empowering the Commissioner to withhold the grant of a patent "for such period or periods as in his opinion the national interest requires." [7] In 1942, Congress extended this authority for the duration of World War II.[8]

These several acts of a temporary nature were replaced by the Invention Secrecy Act of 1951.[9] During floor consideration of the

---

[5] *James* v. *Campbell*, 104 U.S. 356, 357–358 (1881).

[6] Act of Oct. 6, 1917, Public Law 65–80, 40 Stat. 394. It also provided, "When an applicant whose patent is withheld as herein provided and who faithfully obeys the order of the Commissioner of Patents above referred to shall tender his invention to the Government of the United States for its use, he shall, if and when he ultimately received a patent, have the right to sue for compensation in the Court of Claims, such right to compensation to begin from the date of the use of the invention by the Government."

[7] Act of July 1, 1940, Public Law 76–700, 54 Stat. 710.

[8] Act of June 16, 1942, Public Law 77–609, 56 Stat. 370.

[9] Act of Feb. 1, 1952, Public Law 82–256, 66 Stat. 3.

measure, the chairman of the Senate Judiciary Committee, Senator Patrick A. McCarran, declared:

> The existing world situation, together with the signing of the Japanese Peace Treaty and the possibility of a treaty with Germany, indicates that these temporary laws will soon become of no force and effect. It is, therefore, necessary, in order to protect the security of the United States as it may be affected by the disclosure of patents, that positive legislation be enacted for this purpose.[10]

A few months later, the provisions of the Invention Secrecy Act were codified by Public Law 82–593 (approved July 19, 1952) as sections 181 to 188 of title 35, United States Code, with only a few editorial changes.[11]

B. PROVISIONS

Section 181 establishes two groups of inventions. If the Government has a property interest in the invention, the Commissioner of Patents and Trademarks issues a secrecy order on being notified that, "in the opinion of the head of the interested Government agency," publication or disclosure by the grant of a patent on the invention might be detrimental to the national security. The other group consists of inventions in which the Government does not have a property interest. The Commissioner makes these available to defense agencies[12] when disclosure "might, in the opinion of the Commissioner, be detrimental to the national security." If notified that, in the opinion of such agency head, disclosure "would be detrimental to the national security," the Commissioner "shall order that the invention be kept secret and shall withhold the grant of a patent for such period as the national interest requires, and notify the applicant thereof."

An invention "shall not be ordered kept secret and the grant of a patent withheld for a period of more than one year," but the secrecy order is renewable for additional one-year periods when the Commissioner is notified by the agency head who caused the order to be issued in the first place that "an affirmative determination has been made that the national interest continues so to require." However, a secrecy order "in effect, or issued, during a national emergency declared by the President shall remain in effect for the duration of the national emergency and six months thereafter." President Truman had proclaimed a national emergency in December 1950. (The enactment in 1976 of the National Emergencies Act terminated existing declared emergencies, effective two years later.[13])

A secrecy order is appealable to the Secretary of Commerce. An applicant subject to secrecy order who wilfully publishes or discloses the invention it covers can be fined $10,000 or imprisoned for two years, or both. Also, if the invention covered by a secrecy order is

---

[10] Consideration of the bill H.R. 4687. 97 Congressional Record 13670 (1951).

[11] See P. J. Federico, "Commentary on the New Patent Act." 35 U.S.C.A. 42 (1954).

[12] The agencies are "the Atomic Energy Commission, the Secretary of Defense, and the chief officer of any other department or agency of the Government designated by the President as a defense agency of the United States." 35 U.S.C. 181. The Department of Justice was designated a defense agency by Executive Order (see note 9 and accompanying text). The National Aeronautics and Space Act of 1958 designates the National Aeronautics and Space Administration a defense agency. 42 U.S.C. 2457(i) (1976). Defense Department witnesses testified the Central Intelligence Agency is an "agency" under the act but not a "defense agency." See Hearings.

[13] Act of Sept. 14, 1976. Public Law 94–412, 90 Stat. 1255, 50 U.S.C. 1621 (1976).

published or disclosed, or the inventor files a patent application on it in a foreign country without permission, the Commissioner may deem the U.S. application abandoned.

A patent applicant under secrecy order has the right to seek "just compensation" for damage from the agency that caused the order to be issued: damage caused by the order itself and/or for the use of the invention by the Government. He can apply for compensation during a period that begins when he is notified by the Patent and Trademark Office that a patent on his invention would issue but for the secrecy order, and ends six years after a patent issues. If an applicant believes he was not justly compensated by the agency's award, he may sue in the Court of Claims or U.S. District Court. (Unlike the 1917 statute, the Invention Secrecy Act does not require an applicant to tender his invention to the Government to secure his right to compensation.)

1. Executive order decrees Department of Justice a defense agency

Executive Order 10457 of May 27, 1953 (18 FR 3083), designated the Department of Justice a defense agency for purposes of 35 U.S.C. 181 (1976). A senior attorney-adviser in the Office of Legal Counsel of the Justice Department testified at the hearings:

> Although the Department has been designated a defense agency for purposes of § 181, it does not ordinarily review patent applications to determine whether a secrecy order should be imposed. The Department has requested that a secrecy order be imposed on only three occasions. All three requests were made with respect to applications filed in 1952 and 1953 for inventions developed within the Federal Bureau of Investigation.[14]

2. Patent Office regulations

Implementing regulations of the Patent and Trademark Office declare at 37 CFR 5.2(d) that a secrecy order "is directed to the subject matter of the application." [15] They also declare:

> National applications under secrecy order which come to a final rejection must be appealed or otherwise prosecuted to avoid abandonment. Appeals in such cases must be completed by the applicant but unless otherwise specifically ordered by the Commissioner will not be set for hearing until the secrecy order is removed (37 CFR 5.3(a)(1979)).

Assistant Commissioner for Patents Rene D. Tegtmeyer testified:

> Although there is no specific statutory authority for this regulation, it has been promulgated under the Commissioner's general administrative authority, 35 USC 6, for several important reasons. Until recently, few members of the Office's Board of Appeals and its supporting staff possessed the requisite security clearances for handling the appealed cases. The

[14] The Classification of Private Ideas: Hearings Before a Subcommittee of the House Committee on Government Operations, 96th Cong., 2d Sess. (Feb. 28, March 20, and Aug. 21, 1980) (testimony of H. Miles Foy) [hereinafter cited as "Hearings"].

[15] 37 CFR 5.2(d)(1979): Secrecy of Certain Inventions and Licenses to File Applications in Foreign Countries. The PTO announced at 45 FR 37985, 38009 (June 5, 1980) that it has found these regulations "should be revised to clarify procedures and provide up-to-date information relating to these procedures." It anticipated publishing Notice of Proposed Rulemaking in August and a Final Rule in January 1981.

same is true of the judges, officers, and staffs of courts that review decisions of the Office's Board of Appeals.

Also, most applications under secrecy orders are related to Government property interests. The Government is generally reluctant to disseminate classified information to a wide range of persons, even if they have security clearances, nor can a patent issue unless the secrecy order is rescinded. Thus, it was not deemed desirable to expend further efforts and funds in pursuit of a procedure that could not culminate in the prompt issuance of a patent.

Of course, 37 CFR 5.3(a) is worded so that a sufficiently important appeal hearing can be ordered by the Commissioner if the applicant petitions for it. For instance, a delay in the appeal proceeding may prejudice the right to compensation. In such a case, the appeal may be heard.

To my knowledge, however, the only requests for these appeals have been filed by defense agencies for Government owned and prosecuted cases. If an appeal hearing were ordered by the Commissioner and the invention found unpatentable, the application, absent further appeal to the appropriate court, would be considered abandoned. Each secrecy order, however, remains in effect until rescinded or lapsed whether or not the application is abandoned.[16]

Also, the act confers on a patent applicant the right to appeal from a secrecy order to the Secretary of Commerce (35 U.S.C. 181) out these regulations interpose the condition that an applicant's appeal cannot be taken "until after a petition for rescission of the secrecy order has been made and denied" (37 CFR 5.4 and 5.8). Assistant Commissioner Tegtmeyer testified:

> There is really no inconsistency. The right of appeal to the Secretary of Commerce, as provided by statute, must be made under procedures prescribed by the Secretary. The Secretary has prescribed the intermediate step of review by the Commissioner.
>
> It certainly is in the best interests of national defense and the applicant himself to have an appeal heard and decided at the lowest qualified administrative level. The applicant is assured that a decision on his petition for removal of (a) secrecy order will be decided by persons most knowledgeable in a prompt, efficient, and economical manner. The Secretary of Commerce will then have their advice if he later must decide the matter.[17]

3. The Secret Register

On February 18, 1944, President Roosevelt ordered that a register of Government interests in patents and applications for patents be

[16] Hearings. (In written answers to 11 questions raised by the subcommittee after the Feb. 28 hearing, Sidney A. Diamond, Commissioner for Patents and Trademarks, explained, "Because an application is abandoned does not necessarily mean that the invention is. The invention may be disclosed in a pending (continuing or related) patent application. A small, but significant, portion of patent applications are abandoned only after a continuing application has been filed, enabling further prosecution of the same or different aspects of a disclosed invention.")

[17] Id. (In his letter, Commissioner Diamond stated, "Since 1958, according to our records, three secrecy order appeals have been transmitted to the Department of Commerce for decision. However, each secrecy order was rescinded prior to any decision by the Secretary. No decisions have been rendered.")

established in the Patent Office. Executive Order 9424 provided the register "shall be open to inspection except as to such entries or documents which, in the opinion of the department or agency submitting them for recording, should be maintained in secrecy . . . (3 CFR 1943–1948 Comp.)." Patent Office regulations provide under "access to register" (37 CFR Part 7 (1979)):

> The register will not be open to public inspection. It will be available for examination and inspection by duly authorized representatives of the Government, subject to the provisions of § 7.7. Public examination will be restricted to those instruments which the department or agency of origin has so authorized in writing.

Section 7.7 provides for a "secret register":

> Any instrument to be recorded will be placed on a secret record or register at the request of the departmnt or agency submitting the same. No information will be given concerning any instrument in such record or register, and no examination or inspection thereof or of the index thereto will be permitted, except on the written authority of the head of the department or agency which submitted the instrument and requested secrecy, and the approval of such authority by the Commissioner of Patents and Trademarks. No instrument or record other than the one specified may be examined, and the examination must take place in the presence of a designated official of the Patent and Trademark Office. When the department or agency which submitted an instrument no longer requires secrecy with respect to that instrument, it will be recorded or registered anew in the appropriate part of the register which is not secret.

At the hearing, the Assistant Commissioner for Patents testified:

> The Government Register makes the Government's interests easy to determine. A royalty free license to any Government agency allows all other agencies to use the invention royalty free. Therefore, it is important to have an easily usable record of governmental patent rights. Recordation in the statutory register will not suffice, as it can be used only for recording assignments. Licenses, for instance, cannot be recorded in it.
>
> The Government Register is maintained apart from the statutory register established under 35 U.S.C. 261, although some assignments can be recorded in both. The Government Register for recording licenses, assignments, technical data agreements, contracts, or other legal documents conveying interests to the Government in patents and patent applications, has been set up in three parts—departmental interests, public interests, and secret interests. Each part has its own card index and, of course, the instruments recorded are included in that part.[18]

---

[18] Testimony of Rene D. Tegtmeyer.

C. HOW INVENTION SECRECY IS ADMINISTERED

1. The Patent Office Secret Group

The Invention Secrecy Act is administered within the Patent and Trademark Office by the Special Laws Administration Group, also known as "Group 220" and, informally, as "the secret group." Some 30 professionals, including patent examiners, and a clerical staff of 20—all of them cleared to handle atomic energy Restricted Data and "fields of interest" indicated by defense agencies, the Department of Energy and the National Aeronautics and Space Administration. In his testimony, Assistant Commissioner Tegtmeyer explained:

> The Office, as I mentioned, has established an extensive screening system to assure the identification of all patent applications actually or possibly bearing on our Nation's security. Each patent application filed in the Office is processed through the Licensing and Review Branch in the Special Laws Administration Group. Here, patent applications are separated on the basis of their contents into three broad technological categories—chemical, electrical, or mechanical inventions.
>
> Examiners with appropriate security clearances and technological backgrounds inspect each of these applications to determine if they contain national security information. Of course, most security-related applications have already been classified by the Government agency or government contractor prior to filing the application in the Office.
>
> To assist the Office in determining the existence of classified technology that must be kept from the public, the defense agencies have provided us with category or field of interest lists of such technology. Examiners screen each patent application with these lists in mind.
>
> When a patent application involving such a field is found the Licensing and Review Branch puts the application aside and calls it to the attention of each interested government defense agency.[19]

These applications physically remain at the Patent Office, but when they relate to Department of Defense fields of interest a microfiche copy is sent to the department (and retained, if it recommends that a secrecy order be issued).[20]

On average, 300 secrecy orders are issued each year. From 240 to 270 of these protect patent applications which were filed bearing security classification markings. The Assistant Commissioner for Patents testified:

> During fiscal year 1979 the Office received 107,409 patent applications. Of these, 4,829 were thought to contain security-related information and were therefore made available to the

---

[19] Id.

[20] Patent Office regulations (37 CFR 5.1(b) (1979) specify that "[o]nly applications obviously relating to national security," and field of interest applications, are made available; that inspection will be made "only by responsible representatives authorized by the agency to review applications"; that these representatives must sign a "dated acknowledgement of access accepting the condition that information obtained from the inspection will be used for no purpose other than administration of 35 U.S.C. 181–188"; and that copies of appilcations sent out of the Patent Office may not themselves be copied.

> defense agencies for review. Only 243 secrecy orders were issued, of which 200 applications contained security classification markings when filed.[21]

In addition, the Patent Office issued 3,300 secrecy order renewals last year. Under the statutes of 1940 and 1942 and the present law, it was possible for a secrecy order issued in 1940 to remain in continuous effect, without review or renewal, until March 1979. (According to the Secret Group, a patent application filed in 1933 and two others filed in 1936 have been under secrecy order since 1947, and another filed in 1940 has been under secrecy order since 1942. The first three are sponsored by the National Security Agency and the other by the Department of Energy.) The Assistant Commissioner testified:

> The National Emergencies Act became effective on September 14, 1978 and terminated the national emergency declared by President Truman in 1950. The transitional provisions of section 181 implementing the Act required the defense agencies to affirmatively determine for each patent application subject to a secrecy order the need for continuing that order. The Office received a written notice of each determination by the defense agencies and in turn issued any needed notices of renewal.
>
> The review of the outstanding secrecy orders during the transitional period, from September 14, 1978 to March 14, 1979, resulted in 3,300 renewals.
>
> A national emergency was in effect from December 1950 to March 1979 and secrecy orders for patent applications did not need annual reviewing for that entire period. Otherwise, each secrecy order would have been subject to annual review.[22]

When the Patent Office decides that an invention covered by secrecy order is patentable, it sends the applicant a "D–10 Order," or Notice of Allowability, advising that a patent would now issue but for the secrecy order. A high but undetermined percentage of the secrecy orders outstanding a year before the National Emergencies Act took effect involved patentable inventions. This is indicated by the Commissioner's fiscal year report for 1977, which shows 2,802 D–10 Orders as of September 30, 1977. (The number of D–10 Orders declined to 2,778 a year later, and to 2,604 as of September 30, 1979.[23] Asked about rescission of secrecy orders when the inventions claimed have been found unpatentable, Commisioner Diamond wrote:

> The Office has had no reason to keep records that enable us to answer your question and I can only reply in a general way.
>
> There is no relationship between a determination by a defense agency to request the Office to issue or rescind a secrecy order and a determination by the Office concerning patentability. A decision by a defense agency to request issuance of a

[21] Testimony of Rene D. Tegtmeyer in Hearings (C. D. Quarforth, then director of the Secret Group, accompanied Tegtmeyer at the hearings. Quarforth had said he did not have original classification authority, but did have derivative authority to classify documents.)

[22] Id. (The Secret Group reported on July 10, 1980, that the Patent Office issued 2,856 secrecy order renewals in the first nine months of fiscal 1980.)

[23] Commissioner of Patents and Trademarks Annual Report for Fscal Year 1977, 1978, 1979. This is a voluntary report. Commissioner of Patents and Trademarks Annual Report, which appears as part of the Annual Report of the Secretary of Commerce, is required by Public Law 82–593 (66 Stat. 794, 35 U.S.C. 14) (1976), and does not list D–10 Orders.

> secrecy order is based, as I understand it, only on grounds that the disclosure of subject matter (patentable or unpatentable) would be detrimental to the national security. A decision by the Examiner that the claimed invention is patentable is made without regard to whether or not the application is classified or subject to secrecy order.[24]

Until recently, the form used by the Patent Office to notify an applicant of the issuance of a secrecy order did not identify the agency sponsoring the order. Assistant Commissioner Tegtmeyer explained at the hearings why it did not:

> The vast majority of patent applications subject to secrecy orders already contain classification markings when filed in the Office. These are ordinarily filed by the Government or Government contractors. The applicant, contractor assignee, and attorney prosecuting the patent application all know the identity of the Government agency requiring classification markings and subsequently requesting issuance of the secrecy order.
>
> In a few cases the Office issues secrecy orders in applications which when filed did not contain security classification markings. In 1979, for example, 43 such secrecy orders were issued. At the time of filing, the Office cannot know, of course, if the application should have been filed with security classification markings or if any Government agency has an interest in the application.
>
> Several years ago, the Office and the defense agencies began developing a more informative and understandable secrecy order. We were successful and the new secrecy order will be utilized soon. Among its improvements, it will identify the agency requesting the secrecy order.[25]

The new secrecy order format went into service April 1.

2. Defense agencies

The Armed Services Patent Advisory Board, a semi-autonomous interservice unit operated under auspices of the Army Judge Advocate General's intellectual property division, serves as a funnel for defense agency dealings with the Patent Office. Its predecessor, the Army and Navy Patent Advisory Board, was formed in 1940 at the request of the Commissioner of Patents to assist him in implementing the new invention secrecy statute. Neither the Patent Office nor ASPAB keeps records on the extent to which inventors under secrecy order seek and receive "just compensation" from defense agencies in the form of administrative awards, although ASPAB collected awards information from defense agencies for presentation at the hearings (see finding No. 8, above)."

In a pre-hearing interview, an ASPAB official explained that secrecy orders can be viewed as applying to four different situations: (1) to in-house patent applications (from Government employees); (2) to contractor applications, where the invention was made in the course of a classified contract; (3) to the results of Independent Research and

---

[24] Hearings.
[25] Hearings.

Development (IR&D), which is contractor technical effort not required to be performed by a Government grant or contract, but which is reimbursed by the Government indirectly; [26] and (4) to "casement) inventions, made by persons who have neither corporate affiliation nor Government support.

(See historical section of this report for an account of ASPAB's origins and operations.)

D. SOME SECRECY ORDER RECIPIENTS

1. The case of David Pelton Moore

From March 21, 1956 to April 2, 1957, David Pelton Moore was under secrecy order at the request of an agency whose identity never has been revealed to him. Moore is an inventor and patent attorney, now 102 years old, who may have invented solid rocket-propellant. He filed a claim against the United States, seeking "reasonable and entire compensation" for the alleged unauthorized use by the Government of his invention, which was patented in 1964 (this patent was reissued to Moore in 1966 in allowance of its eight claims and some additional claims he included in a 1965 application). Trial has been held, and a decision is pending.[27]

The following outline of Moore's case is drawn from his testimony in the hearings, from a newspaper article he submitted as a hearing exhibit [28] and from court documents:

Moore received the first of his 77 patents in 1904. In 1939, he devised the idea of using rubber as a binder in an explosive composition. In December of that year he drew up a patent application describing the composition and how to make it, then signed the application and had it notarized, but never filed it in the Patent Office.

In 1941, Moore delivered a sample of the material, which he called XL-ite, to the Bureau of Explosives of the American Association of Railroads for testing. When the war broke out he tried to interest the Navy in XL-ite, but the Navy would not test the compound unless he supplied the formula for it, which he declined to do.

In 1948, Moore and Moldex Rubber and Plastics, of New York, entered into a contract for development of his patents. (He never received any royalties from Moldex for this invention.) Later in 1948, Moore and Moldex tried to interest the Navy in XL-ite, by this time also called "Moorite," for use as a propellant. Twenty pounds of it were given to the Navy, free, for testing at Picatiany Arsenal. No sales or orders ever resulted.

From 1950 to 1955, Moore tried to interest Firestone and other large corporations in producing his rubber explosive and propellants. In

---

[26] For a current view of IR&D, see William J. Broad, "Assault on Research Secrets at Pentagon," 207 *Science* 4433, pp. 849–851 (22 February 1980). Broad writes, "To begin at the beginning the Pentagon's IR&D programs pay defense contractors to undertake projects on their own initiative." For background, see Independent Research and Development. Hearings before the Subcommittee on Research and Development of the Committee on Armed Services and the Subcommittee on Priorities and Economy in Government of the Joint Economic Committee. U.S. Senate. 94th Cong., 1st Sess. September 17, 24, and 29, 1975.

[28] Hearings. John M. Barry, "Patent, and Millions, Pending." Washington Post Magazine, Jan. 20. 1980, p 16.

[27] Hearings. Earlier, the Government asked for a separate trial on the issue of abandonment and/or forfeiture of his invention, and Moore won. See *Moore v. United States*, 194 U.S.P.Q. (Ct. Cl. 1977). At the hearings, Moore testified that he is not asserting any claim under the Invention Secrecy Act.

1955, he interested John L. Lewis and the United Mine Workers in financing production of XL-ite. Moore filed his first patent application on this invention on July 27, 1955. After a review of the application, the Patent Office placed Moore under a secrecy order which prohibited him from disclosing the details of his invention to anyone. Moore testified at the hearings:

> The secrecy order prohibited me from disclosing the subject matter of the patent application to others who did not know of the invention prior to the date of the secrecy order. The secrecy order totally ended any interest the Mine Workers had in my invention.[29]

Moore's attorney, who accompanied him, later elaborated:

> The impetus for David's filing his 1955 patent application was the pending deal with the United Mine Workers and a second deal with some people from Baltimore who were going to put up a plant and produce his explosive.
>
> Patent applications are relatively expensive matters, between $2,000 and $3,000 in today's dollars, to prosecute an application to issuance. Therefore, people do not go into them lightly. A lot of people feel that they have to have some kind of commercial application at least pending before they will file.
>
> This, of course, does not apply to large corporations which have almost unlimited funds for filing patent applications. So, the deals David is talking about are deals that he entered into with the United Mine Workers and the people in Baltimore, and the issuance of the secrecy order had the effect of totally chilling, or in his words killing, those deals.[30]

Moore was never given a copy of the Picatinny test report, which had been classified "Secret." It was 19 years later before he learned that the Moorite test had gone well. And it was not until 1970 that a friend of Moore's, visiting the Applied Physics Laboratory in Moore's cause, found additional pages to the Picatinny test report that were still classified: a list of 43 Government laboratories and contractors to whom it had been sent.[31] The Morrite test results had been given to others, but not to Moore.

2. George Davida's cipher device

Dr. George Davida, associate professor of electrical engineering and computer science at the University of Wisconsin-Milwaukee, invented a cipher device that is based on advanced mathematical techniques. On April 21, 1978, he received a secrecy order sponsored by the National Security Agency.[32] A storm of publicity broke, and the order was lifted in June. "If the individual had elected to publish in academic journals," said the director of NSA, "there would have been no question of a secrecy order."[33]

---

[29] Testimony of David Pelton Moore in Hearings.
[30] Testimony of Paul Meiklejohn in Hearings.
[31] Hearings.
[32] Kahn, David. "Cryptology Goes Public," 58 *Foreign Affairs* 154 (Fall 1979).
[33] Id. at 154.

The following contemporary account of the incident is excerpted from the congressional testimony of Frank A. Cassell, then Assistant Chancellor, UW-Milwaukee: [34]

> Professor Davida is a national expert in the area of computer security. His scholarly activity has been aided by a grant from the National Science Foundation. One result was development of a device that protects computers from penetration by unauthorized individuals. Following normal practice in the UW system, Davida signed over patent rights to the Wisconsin Alumni Research Foundation, and WARF applied for a patent in October 1977.
>
> On April 21, 1978, Davida, one of his graduate students and WARF received in the mail a "Secrecy Order From the Patent and Trademark Office." The order stated that disclosure of the principles involved in David's device "might be detrimental to the national security." Davida and everyone else who knew about the device were ordered to say nothing or risk penalties as great as two years in prison and $10,000 fine. Part of the secrecy order permitted Davida to discuss his invention with agents of the U.S. Government and no one else. The secrecy order did not say why the national security was involved, state how long the order would be in effect, or explain any method of appeal.
>
> On learning of Davida's predicament, our chancellor immediately wrote to the director of NSF, requesting his assistance. Before he could respond, news of the order was printed in the Milwaukee Sentinel and picked up by the New York times. Within days the story was carried throughout the U.S. and attracted journalistic interest in Canada and Great Britain. On June 15 a one-paragraph document titled "Rescinding Order" was received by Prof. Davida from the Patent Office.

Cassell said "disturbing questions remain":

> Should the executive branch of Government be able to prevent a citizen from speaking or publishing without some involvement by the courts? Should the executive branch of Government be able to invoke the claim of "national security" without demonstrating that our national security was genuinely threatened? Should defense or intelligence agencies be able to interfere with or inhibit academic research through the patent process? Is censorship an appropriate function of the Patent and Trademark Office? Who will prevent abuses of the secrecy order concept that could frighten professors and stifle research in areas someone in a defense or intelligence agency opposes? [35]

At this year's hearing on the Classification of Private Ideas, Davida characterized the secrecy order as "worrisome for a number of reasons," and explained:

---

[34] Government Patent Policies: Institutional Patent Agreements. Hearings Before the Subcommittee on Monopoly and Anticompetitive Activities of the Select Committee on Small Business. U.S. Senate. 95th Cong., 2d Sess. May 22, 23, June 20, 21, and 26, 1978. Part I, p. 770.

[35] Id., pp. 771–772.

1. The university environment is not one in which secrets can be kept. The first time that I knew anything about the secrecy order was in a telephone conversation, with several students waiting to see me and who couldn't help but listen to the conversation.

2. Questions arose about what responsibilities I had to keep the material secret. The technical report may have been sent out to just about anyone who requested it from the departmental secretary. I had also included some of the material in a proposal to the National Science Foundation. Thus, many people, whom I didn't know, may have had access to the material. Yet, there was a requirement that I report the names of individuals that I had sent the report to. (This in itself was bothersome, since I would in effect be involving other colleagues in the secrecy order.) There was also the matter of the $10,000 fine and the two-year jail term for noncompliance. I was worried about having to prove that I did not leak the report.[36]

Discussing the NSA director's remark, and whether choosing to patent rather than publish elevated profit motive over academic freedom. Davida said the laregst share of profits from any patent obtained by the Wisconsin Alumni Research Foundation would go to the University, adding:

> Furthermore, one can argue that profit from such things as patents and stocks held by universities enhances rather than diminishes academic freedom, since the profits can be used in the Wisconsin system) to fund research, thus freeing the university from having to seek additional funding from State or federal sources.[37]

3. Squelching the voice scrambler [38]

On or about the day Professor Davida received his secrecy order, the NSA was obtaining one on the patent application for a voice scrambler that would let radio and telephone users chat without being overheard by others. The inventors, Carl R. Nicolai, William M. Raike and David L. Miller, had filed their application on October 20, 1977.

The Patent Office lifted the secrecy order on October 11, 1978, after Nicolai had charged that the order "appears part of a general plan by the NSA to limit the privacy of the American people. They've been bugging people's telephones for years and now someone comes along with a device that makes this a little harder to do and they oppose this under the guise of national security." [39]

During the week of February 10, 1980, the inventors received Patent No. 4,188,580 on their device, which they contend could protect telephone conversations, business radio transmissions and other communications at a much lower cost than the voice scramblers now on the market.

---

[36] Testimony of George Davida in Hearings.
[37] Id.
[38] See generally, Stacy V. Jones, "Message Scrambler Devised," New York Times, weekly patents column, Feb. 16, 1980; "Inventors Given Patent That NSA Had Blocked," Washington Post, Feb. 17, 1980, at A8.
[39] D. Kahn, supra note 26 at 155.

When he testified at the hearings, Admiral B. R. Inman, Director, NSA, said the Davida and Nicolai situations exemplified "not a faulty law but inadequate Government attention to its application." He summarized NSA involvement in the former as "a very well meaning attempt to hold the line that had clearly already been passed by and a situation in which a middle level employee could say no." Inman said of the latter case:

> There I was faced with a split decision inside NSA over whether the Nicolai invention represented a threat. From dealing day by day with the Invention Secrecy Act, you have to make a quick, snap decision.[40]

In the Nicolai matter, Inman added that

> the interesting side of that one is that the same day I heard from the lawyer asking questions about our request for a secrecy order, I also heard from the public affairs representative seeking to draw maximum publicity to the invention. We have clearly given a fair impetus to the marketing prospect for that invention with the very substantial efforts of the public relations persons to build a case that if it is good enough that NSA might have wanted to restrict it, clearly it is good enough that you ought to buy it.[41]

E. LEGAL ASPECTS OF INVENTION SECRECY

1. The Government's exercise of police powers

The Atomic Energy Act of 1954 and the National Aeronautics and Space Act of 1958 either prohibited or curtailed the grant of private patents in these domains, and directed the Commissioner to screen all applications for inventions useful in atomic energy or which appear "to have significant utility in the conduct of aeronautical and space activities."

One analyst, who is an attorney and patent examiner, believes these statutes and the Invention Secrecy Act represent "a reasonable exercise of the police power." He writes:

> Access to confidential information belonging to private citizens under the aforementioned circumstances represents a reasonable exercise of the police power to protect the national security and the proprietary rights of the government. In the interest of self-preservation, a government must assume power to protect itself against, as by the suppression of, the disclosure of potentially destructive weapons and other instruments of warfare. An applicant for patent suffers no damage by reason of the government's mere inspection of his invention. Indeed, some form of governmental inspection is a condition precedent to every grant of patent. Actual use thereof by the government or damage suffered by the inventor by reason of the government's suppression, however, constitutes a taking of private property for public use—an exercise of the power of eminent domain, entitling the property

[40] Hearings.
[41] Id.

> owner to just compensation, as provided for by the Fifth Amendment.[42]

In his view, these provisions for suppression of information affecting the national security "are but a specific application of the power of eminent domain at the patent application stage." He adds:

> The Fifth Amendment, impliedly sanctions the taking of private property for public use, by requiring only that just compensation be paid therefor. Of course, public use is not defined by the Constitution. Few, however, would dispute that articles intended for use directly by the government and/or its agents fall within the meaning of a public use. Moreover, public use includes not only what is necessary for national security but also what is needed for maintaining public health and safety.[43]

As noted, the Invention Secrecy Act confers a right to compensation upon the applicant whose patent is withheld by a secrecy order. The right begins on the date the applicant is notified that a patent would issue but for the secrecy order, and six years after the patent issues. The applicant has two ways of proceeding as described by Donald S. Chisum, University of Washington, Professor of Law:[44]

1. The first is to apply to the agency causing the order to be issued for a settlement agreement and, in case of a less-than-satisfactory award, to file suit in either the Court of Claims or the District Court in which the applicant resides.

2. The second is to await removal of the secrecy order and issuance of the patent and file suit in the Court of Claims.

Chisum cites three problems of interpretation that have arisen about these alternate ways of securing compensation: (1) where the applicant under a secrecy order applies for an administrative settlement and the agency refuses to make any monetary award;[45] (2) where the applicant files a court action seeking compensation under the first avenue prior to issuance of the patent and while the secrecy order is still in effect;[46] and (3) where the applicant under a secrecy order files an action in district court to recover compensation for use by the Government of the invention under an implied license—both before and after issuance of the patent.[47]

2. First amendment questions

In 1978, the Office of Legal Counsel of the Department of Justice sent a memorandum opinion to Dr. Frank Press, Science Adviser to the President, on the constitutionality under the First Amendment of restrictions imposed on public crytography by the International Traffic in Arms Regulations (ITAR)—that is, on dissemination of cryptographic information developed independently of Government supervision or support by scientists and mathematicians in the private sector.

---

[42] Peter D. Rosenberg, "Patent Law Fundamentals" 177 (1977).
[43] Id., p. 178.
[44] Donald S. Chisum, 1 "Patents: A Treatise on the Law of Patentability" 1–195 to 1–199 (1978).
[45] See, e.g., *Robinson* v. *United States*, 236 F.2d 24, 110 U.S.P.Q. 164 (2d Cir. 1956).
[46] See, e.g., *Halpern* v. *United States*, 258 F.2d 36, 118 U.S.P.Q. 386 (2d Cir. 1958).
[47] See, e.g., *Farrand Optical Co.* v. *United States*, 317 F.2d 875, 138 U.S.P.Q. 490 (2d Cir. 1962).

This opinion, signed by Assistant Attorney General John M. Harmon, remarked on the linkage between regulation of public cryptography and issues of Government control over dissemination of technical data (discussed in the export control policy section of this report). The opinion observed in an early footnote:

> Our research into the First Amendment issues raised by Government regulation of public cryptography led tangentially into broader issues of Government control over dissemination of technical data. Those questions are numerous, complex, and deserving of extensive study, but are beyond the scope of this memorandum.[48]

It found little judicial guidance on First Amendment questions about Government restrictions on privately generated data. There was one published decision addressing a First Amendment challenge to the ITAR (a second has been published since the opinion was written). Beyond that, it said, "Our research into areas in which Government has restricted disclosure of nongovernmental information provided little additional guidance." It continued:

> Perhaps the closest analogy to controls over public cryptography are the controls over atomic energy research. Under the Atomic Energy Act of 1954, 42 U.S.C. 2011 et seq. (1970), all atomic energy information, whether developed by the government or by private researchers, is automatically classified at its creation and subjected to strict nondisclosure controls. Although neither the Atomic Energy Act nor its accompanying regulations establish formal procedures for prior review of proposed atomic energy publications, the Atomic Energy Commission (whose functions are now divided between the Nuclear Regulatory Commission and the Department of Energy) has been empowered to maintain control over publications through threat of injunction or of heavy criminal penalties, two potent enforcement tools provided under the Act, 42 U.S.C. 2271–2277, 2280. It does not seem, however, that the broad information controls of the Atomic Energy Act have ever been challenged on First Amendment grounds. Our search for judicial decisions in other areas in which the government has imposed controls over the flow of privately generated information was equally unavailing. (citations omitted) [49]

It discussed these other areas in a footnote:

> For example, it does not appear that the broad controls over exports of technical data and related information under the Export Administration Act of 1969; 50 U.S.C. App. 2401 et seq. (1970), and accompanying regulations have been judicially tested on First Amendment grounds. Nor have the provisions of the patent laws restricting patentability of inventions affecting national security, 35 U.S.C. 181 et seq.

---

[48] Memorandum opinion dated May 11, 1978, from John M. Harmon, Assistant Attorney General, to Dr. Frank Press, Science Adviser to the President. The opinion, never made public by the Justice Department, was incorporated in the hearing record and declared a public document on Feb. 28, 1980. See Hearings (hereinafter cited as "OLC Opinion").

[49] Id.

(1970), nor governmental restrictions on communications with Rhodesia, 22 U.S.C. 287c (1970); Exec. Order No. 11,322.[50]

At the hearings, the Justice Department witness concluded his prepared statement by noting the subcommittee had posed a series of questions about the power of the Government to acquire "proprietary interests" in intellectual property important to the national defense, including: How does the Government acquire such a "proprietary interest"? Does the Government take title? Does the Government assert a peacetime power of eminent domain over intellectual property absent some statute that authorizes involuntary acquisition? He responded:

> These are complicated questions. To simplify the problem, let me shift the focus of the inquiry to some degree. I have suggested that property law concepts do not always provide infallible guidance when we attempt to discover the nature and limits of the Government's powers in this area. I want to renew that argument here. The essential problem is not to determine how and when the Government may obtain "title" or other incidents of "ownership" in intellectual property in the private-law sense, but to determine how and when the Government may assert a right to prevent or punish the dissemination of defense-related information in the possession of private individuals, preventing them from using it or exploiting it for their own private purposes. How and when may the Government acquire and assert such a right?
>
> Recognizing the complexity of the subject, the short answer is the following: The Government may acquire and assert such a right under a properly drafted criminal statute where the danger presented by the disclosure is sufficient to justify the prohibition. Absent a statute, the Government may in rare circumstances assert such a right in a suit for an injunction against a disclosure that will present a grave danger to the national defense. Absent a grave danger, the Government may in some circumstances enjoin a disclosure of information protected under an agreement or special relationship between the Government and the individual in question. As against a stranger, in the absence of a statute or an extraordinary danger, the Government may have no remedy at all.[51]

The Department also was asked whether any provision of the Invention Secrecy Act suffers constitutional infirmities under the First or Fifth Amendments, but witness Foy testified that the Department "has thought it wise to follow a rule of self-restraint in expressing public views on constitutional questions presented by the statutes we are called upon to enforce." He gave three reasons for the rule, and then said:

> The present case is an appropriate case for the application of this rule. As regards the First Amendment questions, it is

---

[50] Id.
[51] Testimony of H. Miles Foy in Hearings.

> perfectly true that any flat prohibition on private speech raises an issue under the First Amendment, but we are dealing here with a prohibition, § 186, that has never been tested. There has never been a prosecution under § 186. We have no judicial opinion to guide us. In advance of litigation, undisciplined by facts, the expression of views on the First Amendment issues that might be presented by a prosecution under this statute would be difficult in any event and would be either self-serving or prejudicial from the standpoint of the Department's duty to enforce the statute. As regards the Fifth Amendment issues, I note simply that the statute provides both an administrative and a judicial remedy for damages caused by the secrecy procedure.[52]

3. Compensation for intellectual property

In a subsequent footnote, the memorandum opinion of May 1978 from the Office of Legal Counsel acknowledged that a question which would arise from complete governmental control over cryptographic information "is whether the Government would be required under the Fifth Amendment to pay just compensation for the ideas it had effectively 'condemned'." It continued:

> For example, the patent and invention provisions of the Atomic Energy Act require the Government to pay for patents which it revokes or declares to be affected with the public interest. A cryptographic algorithm, however, would not appear to be a patentable process. And it is unresolved whether copyright protection is available for computer software. We are therefore uncertain as to the status of cryptographic ideas under the Fifth Amendment. (citations omitted) [53]

As noted, the right to compensation set forth in the Invention Secrecy Act differs in two respects from what preceded it: The applicant need not tender the invention for Government use in order to secure the right, and need not wait until a patent actually issues before seeking compensation.

However, staff interviews of Armed Services Patent Advisory Board officials indicate that defense agencies construe the act in such a way that the right to compensation is often more illusory than real. Staff was told that defense agencies do not make administrative awards for secrecy order damage claims where the invention was suppressed but not used by the Government and the Government was the sole intended market for the invention.

Further, it is not clear whether the patent applicant bears the entire burden of determining the market value of his intellectual property in support of a claim for compensation, as the owner of real property does in an eminent domain proceeding, or how this value can be determined for inventions having commercial potential when the applicant is barred by secrecy order from disclosing the invention to

---

[52] Id.
[53] OLC Opinion at 15, n. 20, printed in Hearings.

prospective licensee.[54] Permits may be granted authorizing disclosure of the information to specified persons, but that raises the marketing question of how a person having no knowledge of the invention can be told enough about it after the secrecy order issues to elicit his interest in becoming a permittee.

At the hearings, the deputy general counsel of the Department of Energy testified about its compensation practices under the Invention Secrecy and Atomic Energy Acts:

> In regard to DOE procedures for evaluating requests from inventors for compensation under the Atomic Energy Act, Section 157 of the Atomic Energy Act (42 USC 2187) provides for the designation of a Patent Compensation Board to consider applications for compensation, awards and royalties based upon claims under the Atomic Energy Act. In addition, the Board has been given authority to consider claims based upon the Invention Secrecy Act (35 USC 183). Since its inception, the Board has considered 40 applications. Thirty-eight of the 40 applications were for awards and just compensation under the Atomic Energy Act. Two applications of the 40 included claims for compensation because of PTO secrecy orders. In the first application, the Board found the claim without merit. In the second application, claims were made for compensation and award under Sections 151, 153 and 157 of the Atomic Energy Act of 1954, as well as under 35 USC 183. The claim was settled for $120,000, and all rights in and to the invention were assigned to the Government without stipulation of which of the several allegations were relevant to the settlement.[55]

F. SUMMARY

The Invention Secrecy Act has endured nearly 30 years without a challenge on First Amendment grounds. In the last 40 years (through July 3, 1980), the Armed Services Patent Advisory Board and its predecessor, the Army and Navy Patent Advisory Board, have requested 41,432 secrecy orders.[56] Indeed, the patterns of practice in invention secrecy are 40 years old. The groundwork was laid before Pearl Harbor.

D. Recommendations

EXECUTIVE

1. The President

(a) Revoke President Roosevelt's Executive Order 9424 of February 18, 1944, establishing a secret register at the Patent and Trademark Office. A subcommittee staff inspection of the secret register, described in a memorandum printed with the hearings, found it to be the classi-

---

[54] The Internal Revenue Service's engineering and valuation branch appraises property—including patents—for gift and inheritance tax purposes. A recent newspaper article asked, "How, for example, do you affix a value to a patented idea—by definition unique—which no one's tried yet to market?" It continued: "You make an educated guess," explains Geoffrey Taylor, chief of the engineering and valuation branch. "It's definitely an art and not a science." See "IRS Appraisers Fly the Art of Educated Guesswork," The Washington Post, July 19, 1980.

[55] Testimony of Eric J. Fygi in Hearings.

[56] Information from the ASPAB secretary on July 21, 1980.

fied attic of the United States, not used by anyone for the last seven years. Since the secret register clearly is no longer needed, neither is the executive order which established it.

(b) Revoke President Eisenhower's Executive Order 10457 of May 27, 1953, designated the Department of Justice a defense agency for purposes of the Invention Secrecy Act. At the hearings, the subcommittee received testimony that the Department does not routinely scan patent applications, has no field-of-interest list on file at the Patent Office, and has been sponsoring three secrecy orders since 1952–53 on Federal Bureau of Investigation employee inventions, which it can do without enjoying "defense agency" status. Unneeded executive orders should be expunged.

(c) Replace the phrase "proprietary interest" in President Carter's Executive Order 12065 of June 1978 on National Security Information, with the phrase "property interest" used in the Invention Secrecy Act. The executive order properly exempts the Invention Secrecy Act from its purview, but the Government ownership standard for secrecy order purposes and classification purposes should be the same. By using "proprietary interest," the Government sets an easy ownership standard for itself and facilitates classification of private ideas.

2. Patent and Trademark Office

(a) Start making a complete annual report to Congress on invention secrecy operations without waiting for amendment of Title 35, United States Code, or Department of Commerce order requiring it. Invention secrecy is sufficiently important to have spawned a patent office within the Patent Office to administer it. The report should include: the numbers of secrecy orders issued and renewed; list of numbers sponsored by agency; breakdown of carryover secrecy orders rescinded since the National Emergencies Act took effect in September 1978; breakdown of cases under the 3-year rule (35 U.S.C. 267) and every other statutory rule—or rule promulgated under 35 U.S.C. 188—seen as authorizing national security handling of patent applications; estimated cost to the Patent Office and all other agencies of implementing the Invention Secrecy Act; narrative statement on the quality of defense agency technical reviews of patent applications and of petitions to rescind secrecy orders; listing of secrecy orders more than 10 years old, by age; synopsis of statutory access acknowledgement lists, to show on average how many persons examine each application in connection with invention secrecy; breakdown of foreign origin cases; number of applications sealed on grounds that disclosure would jeopardize national security; and statement of progress on proposed changes in regulations and forms implementing invention secrecy.

(b) Make special one-time report to Congress on its record-keeping authorities and practices with respect to patent applications. When does the Patent Office transfer records to the National Archives? Where and when does the Patent Office retire its records?

3. General Services Administration/Information Security Oversight Office

(a) The Information Security Oversight Office (ISOO), established within the General Services Administration by Executive Order 12065 to oversee agency compliance in national security classification matters,

should review the propriety of classification markings placed on patent applications in these two situations:

1. All patent applications filed with the Patent Office in fiscal year 1980 bearing classification markings, whether the classifying official had original or derivative classification authority. (In 1979, 200 of the 243 secrecy orders issued by the Patent Office applied to applications which were filed bearing classification markings.); and

2. All patent applications not bearing security classification markings which were referred by the Patent Office to defense agencies for review and were returned to the Patent Office bearing classification markings. (This number presumably is smaller than the 43 applications received by the Patent Office not bearing classification markings on which secrecy orders ultimately were issued. However, it is conceivable that some patent applications might be classified by defense agency reviewers and returned to the Patent Office without a request that a secrecy order be issued.)

This review should determine in each case what part of the application was or came to be classified: the claim made for the invention, the description of the invention itself or the prior art cited. It should determine how many applications were classified by contractors exercising derivative classification authority, and should review declassification practices with respect to rescission of secrecy orders.

4. Department of Defense

(a) Within the Office of the Secretary of Defense (OSD), relearn the Invention Secrecy Act so that it will understand how much invention secrecy authority has been delegated and can assess how it is exercised, and also so that it will have a knowledgeable witness to testify on behalf of OSD when congressional committees so request.

(b) Make a one-time report to Congress on the intellectual property aspects of contractor inventions made pursuant to Independent Research Development (R&D), where the work is indirectly funded by the Government but is not required to be performed in fulfillment of a contract. Report is to include explanation and authority for the allocation of rights in such inventions between the Government and the contractor, and an explanation, with examples, of the frequency and reason for imposition of secrecy orders on patent applications covering such inventions. Also, the report should include statement of current Executive Branch position and activity on Recommendation I–13 of the Report of the Commission on Government Procurement ("Eastablish a remedy for the misuse of information supplied to the Government in confidence"), inasmuch as the General Accounting Office issued its final assessment of the commission's recommendations in May 1979 (PSAD–79–80).

5. All agencies sponsoring secrecy orders

(a) Should reexamine their procedures for receiving and evaluating secrecy order damage claims from applicants pursuing their statutory right to just compensation. Agencies should temper their response to such claims in the awareness that they typically request secrecy orders on the basis of classifiability of the information in an application, while the applicant has to prove patentability to qualify for just compensation.

JUDICIAL

1. U.S. Court of Claims

(a) In response to a general congressional request, as in a congressional reference case under 28 U.S.C. 2509 (1976), the chief commissioner of the Court of Claims should report to Congress on the frequency and fairness of Invention Secrecy Act claims and settlements. Report should include: Does the act sufficiently furnish and define the basis of a patent applicant's claim? In the court's experience, do applicants generally (1) first seek but fail to obtain an administrative award, (2) obtain an administrative award they deem not to be just compensation, or (3) bring action in the Court of Claims without first seeking an administrative award from the agency sponsoring the secrecy order? Does the Government acknowledge in paying claims and making settlements that applicants can and do suffer damages as a result of the secrecy order itself? Do agencies use or could they use an expert and independent board of appraisers (akin to what the Internal Revenue Service attempts) to help determine the amount of damages an applicant incurs due to a secrecy order?

LEGISLATIVE

1. General Accounting Office

(a) Audit the Government Register at the Patent and Trademark Office, which exists "for recording licenses, assignments, technical data agreements, contracts or other legal documents conveying interests to the Government in patents and patent applications" (Patent Office testimony in the hearings). Determine:

1. Are there assignments to the Government containing reversionary clauses which return those rights to the applicant/patentee after a stipulated time?

2. What kinds of right-in-data agreements are entered here?

2. The Congress

(a) Should re-examine and reconsider the Invention Secrecy Act in light of the following:

1. Make the necessary findings and declaration of public policy that would justify the exercise of invention secrecy powers in peacetime;

2. Strengthen the patent applicant's right to receive just compensation for damages suffered as a result of imposition of a secrecy order;

3. Change the basis for issuance of a secrecy order from the opinion of an agency head that disclosure might or would be "detrimental to the national security," to a more demonstrable standard of damage to the national defense;

4. Require that an agency head personally request issuance of a secrecy order (rather than delegate the authority), or make the request reviewable and cancellable;

5. Clarify what constitutes a Government "property interest" in a patent application, especially in view of pending legislation that would generally allow contractors to acquire principal rights in inventions they make as a result of federally funded research

and development, while reserving lesser—and often delayed—rights to the Government;

6. Consider giving the Commissioner of Patents and Trademarks the discretion to refuse to issue a secrecy order requested by a defense agency; and

7. Curtail the authority agencies enjoy to "separately issue rules and regulations" for invention secrecy purposes. Testimony at the subcommittee hearings established that this authority (35 U.S.C. 188) is the source of (A) the Patent Office requirement that an applicant under secrecy order first petition the sponsoring agency for rescission before pursuing his statutory right of appeal to the Secretary of Commerce, and of (B) the Armed Services Patent Advisory Board rule that all three services represented on it must approve the rescission of a secrecy order, though it only takes one to request an order.

E. Historical Section

During World War II the Patent Office employed six extraordinary measures to ensure the security of certain issued patents and thousands of patent applications, overlaid upon its standard practice of guaranteeing the confidential handling of all patent applications. It restricted the public availability of some issued patents by impounding them, which meant disallowing inspection of the file wrapper and withdrawing sale copies and, in varying degree, discontinuing inspection of patent examiners' copies, search room copies and bound volumes. The other five, which could be used interchangeably or in combination, pertained to patent applications:

Super Secrecy—applications sealed without examination by anyone.

Special Handling—applications examined under extra secrecy precautions.

Blue Slip—applications forwarded to the Patent Office War Division at time of filing, a temporary form of Special Handling.

Secrecy Orders—applications kept from issue or other disclosure under the 1940 invention secrecy statute.

Three-Year Rule—applications assigned to the Government kept from issue or abandonment.

Except for Super Secrecy and Special Handling, which were mutually exclusive, these five security procedures could occur in any combinations on the same application. They could also occur in combination with extraordinary measures taken outside the Patent Office, resulting in a complete blackout of information. That is what happened to radar.

WORLD WAR II RADAR SECRECY

On July 16, 1943, the military Combined Chiefs of Staff agreed "that immediate steps would be taken to stop all public dissemination of radar information in the United States and in the British Commonwealth and that recommendations to this effect should be made forthwith to the appropriate authorities of the Governments concerned." On July 24, President Roosevelt authorized—and there was issued—a classified directive reading:

1. It is the present policy of this Government to suppress the dissemination of information on radar.

2. You are directed to cause all divisions and agencies under your control, which release information, to comply with the policy set forth above.[57]

In Germany on July 16, a Reich Radar Research Authority was founded "to supervise an expansion of the German radar and high-frequency electronics industries, and organize all fundamental research." [58] In Britain the day before, a final conference had been held to discuss use of a new tactic—codenamed "Window"—to jam the German radar system. And on July 24, the date of the President's directive, the British opened the Battle of Hamburg:

> By midnight, the whole bomber stream was assembled over the North Sea, a mighty phalanx of 791 aircraft—347 Lancasters, 246 Halifaxes, 125 Stirlings and 73 Wellingtons—two hundred miles long and twenty miles wide.[59]

On that raid, the British dropped 40 tons of "Window"—92 million strips of aluminum foil.[60]

The Royal Air Force was not the first to jam radar with metal strips. In May 1943, in the battle for the Solomon Islands, the Japanese Navy started to use paper-backed metal screening 75 centimeters long—half the wavelength of American gunnery-control radar sets—to shield its bombers during night attacks on Guadalcanal.[61] Also in May, Reichsmarschall Herman Goring, after reading a report on a captured, powerful British ground-looking *H2S* unit, reassembled and analyzed by Telefunken engineers, remarked:

> We must frankly admit that in this sphere the British and Americans are far ahead of us. I expected them to be advanced, but frankly I never thought that they would get so far ahead. I did hope that even if we were behind we could at least be in the same race.[62]

In the midst of the wartime round of electronic measures and countermeasures, the United States adopted a policy of suppressing information about radar. The policy laid down by the Joint Chiefs of Staff was implemented in an August 1943 directive from the Adjutant General of the War Department to all commanding generals:

1. Officers of the United States Army irrespective of rank or position shall under no circumstances include reference to radar in any release if information, in speeches or other public communications.

2. All accredited correspondents within the jurisdiction of the United States Army shall be requested to omit all reference to radar in dispatches or articles originated by them.

3. Research, development and procurement agencies under War Department control will inform all contractors involved

---

[57] Batch X.
[58] Alfred Price, "Instruments of Darkness. The History of Electronic Warfare." New York, Charles Scribner's Sons (1977), p. 148.
[59] Id. at 153.
[60] Id. at 158.
[61] Id. at 142.
[62] Id. at 136–137.

in the manufacture of radar equipment that they are specifically requested to refrain from any references whatever to radar in their advertising material.[63]

It was to be a total blackout.

RADAR PATENT SECRECY

To cloak the subject even more, the Army and Navy Patent Advisory Board, interservice adviser on invention secrecy, prepared a letter for the Commissioner of Patents requesting "that all applications for patents which mention the word or which disclose radar equipment and methods" be submitted to the board. The letter continued:

> Furthermore, it is requested that all applications in the above category that have already once been submitted and disapproved be resubmitted. It is also requested that all applications falling in the above category which have once been placed under a secrecy order and later rescinded to be resubmitted to the board.[64]

Indeed; use of secrecy orders—by which applications were kept from issue or other disclosure—was only one of six wartime Patent Office procedures relating to security. Two others were "Super Secrecy," the sealing of applications without Patent Office examination, and "Impounding," which blocked public access to issued patents. When a patent was impounded, inspection of the file wrapper and sale of soft copies was discontinued Impoundment could also mean discontinuing inspection of examiners' copies, search room copies and bound volumes.

As an example of regard for radar invention secrecy, consider this analysis of October 30, 1945, for the Office of Scientific Research and Development by John C. Batchelor at the MIT Radiation Laboratory, of the need for maintaining secrecy orders on a patent application by Dr. Otto Halpern and two others assigned to DuPont:

> The subject applications relate to a surface treatment for radar targets designed to render them non-reflecting to radar energy and was a project which was held under the greatest possible security restraint for the duration of the war. The original development appears to have come from Dr. Otto Halpern in the Radiation Laboratory but by OSRD contract, and later by Navy contract DuPont was active in the devlopment.
>
> Dr. Halpern has in the past indicated to me that he considers the commercial rights to his method and material to have significant value, but he has not been able in response to my questioning to be specific on the point. On the other hand, the military significance of "black body" treatment goes considerably beyond mere function of accomplishing radar camouflage and enters the field of target identification, such as in the Radiation Laboratory "Sambo" project and perhaps others.

---

[63] Batch X.
[64] Batch X.

> We have followed closely the attempts of Germany to achieve the results accomplished by our materials, and we are aware of the substantial extent to which they fall short of achieving the desired result.
>
> In view of the military importance of the material disclosed in these three applications, the failure of our enemy to achieve similar results and the absence of immediate commercial significance, we recommend that secrecy be maintained in these three applications.[65]

In *Instruments of Darkness*, Alfred Price write that Germany's electronics genius, Dr. Hans Plendl, "devoted considerable theoretical research to the possibility of making U-boats 'invisible' to centimetric radar by coating them with a special material," and that he reported in December 1943 having achieved a 50-percent reduction in a U-boat's radar reflection. Adds Price:

> The research was generally referred to as "black U-boat" work. In spite of Plendl's optimistic report, and the capture of full information on his research after the war, there still is no such thing as an "invisible" submarine.[66]

Although the radar concept dates to April 30, 1904, when the Royal German Patent Office granted a patent to Christian Hulsmeyer for a device he called the "Telemobiloscope," the ordinary man in the street in Britain and Europe had never heard of radar as of the summer of 1942.[67] Nor did anyone have a monopoly on the idea:

> Radar, like most of the major technological advances during the twentieth century, did not result from a sudden and inspired line of thought pushed to the point of fulfillment by one inventor. As with the other great innovations, the basic idea preceded the invention by several decades, and it was only when certain special means had been developed that its realisation became practicable. Again, as with the other great inventions of this century, once the background work was complete development proceeded independently in several nations simultaneously.[68]

Nor was the man in the street likely to learn anything of American developments in radar after July 1943. The memo to staff from the chief of the Signal Corps review branch announcing the policy on radar included these instructions:

> Clear no radar publicity whatever that originates in any agency of either of the armed forces. In such refusal you will be acting by authority of the Joint Chiefs of Staff.
>
> Refuse to recognize the principle of prior publication where radar material is involved.
>
> Strike out all references to the fact that radar was used in any specified engagement.

---

[65] Batch L. (Halpern's application remained under secrecy order until 1959. His suit for damages was settled in about 1959, during the course of litigation. The claim for damages for use of the invention while it was under secrecy order was settled by payment of $305,000. See letter of March 14, 1980, to the subcommittee chairman from William G. Gapcynski, Chief, Intellectual Property Division, Office of the Judge Advocate General, Department of the Army, in Hearings.)

[66] A. Price, supra note 2 at 143.

[67] Id. at 56, 91.

[68] Id. at 55.

Disapprove publication of any pictures, sketches or diagrams of radar installations or parts.

Delete all controversial material involving national or personal credit for the invention or development of radar.[69]

OTHER TOOLS OF WAR

Radar became a special case, as were atomic energy and cryptology, but thousands of technical secrets were kept, ranging from petroleum and synthetic rubber technology to torpedoes and nylon (when it came to be used in parachutes). In December 1943, the Signal Corps suggested to the Commissioner of Patents that its experts be allowed to review "all applications of Teletype Corporation relating to Teletype machines and components thereof." It appended a list of persons who had assigned their patent rights to Teletype Corporation and designated five of them as "the most probable inventors." [70] If there was doubt about the potential military applicability of the invention disclosed in a patent application, a secrecy order was issued for safety's sake. The number of secrecy orders in effect climbed from 727 on December 15, 1941, to 8,293 as of December 31, 1944.[71]

Congress authorized invention secrecy in a World War I statute, declaring that "whenever during a time when the United States is at war the publication of an invention by the granting of a patent might, in the opinion of the Commissioner of Patents, be detrimental to the public safety or defense or might assist the enemy or endanger the successful prosecution of the war he may order that the invention be kept secret and withhold the grant of a patent until the termination of the war." [72] Congress broadened this authority in 1940 by deleting the requirement that the United States be at war and empowering the Commissioner to withhold the grant of a patent "for such period or periods as in his opinion the national interest requires." [73] In 1942, Congress extended this authority for the duration of World War II.[74]

At the request of the Commissioner of Patents, the Secretary of War and the Secretary of the Navy created the Army and Navy Patent Advisory Board (ANPAB) in August 1940, giving it the dual role of advising the Commissioner and of "bringing to the attention of the Military Departments, inventions in the form of patent applications which may pertain or be applicable to the national defense." [75] ANPAB functioned throughout the war, using over 300 technical personnel of the War and Navy Departments to review patent applications, and recommending 4,703 of the 8,152 secrecy orders in force in June 1945.[76] It continued into the postwar period, was renamed the Armed Services Patent Advisory Board (ASPAB) in 1948 and exists to this day.

As a 40-year-old interservice entity, ASPAB claims a niche at the National Archives. Officially it is Record Group 334, "Records of the Armed Services Patent Advisory Board 1940–45." It is two linear

[69] Batch X.
[70] Id.
[71] Batch O–C and Batch M.
[72] See note 2 supra.
[73] See note 3 supra.
[74] See note 4 supra.
[75] Batch C–2 and Batch D–1.
[76] Batch C–2.

feet of records, predominantly from the war years but reaching to 1953, with a few documents to 1956 and three strays dated 1961. It is an odd lot.

The records consist mainly of correspondence, principally with the Patent Office, and of minutes of ASPAB meetings. They include memoranda, and file copies of correspondence exchanged by others. They include drafts of letters—for example, of the request to the Patent Office to reexamine patent applications involving radar—with no indication whether the letter was actually sent. Some were classified "Secret"—an excerpt from the Joint Chiefs' radar secrecy policy statement, for example—or "Confidential" or "Restricted," and bear the markings of periodic downgrading.

They do not constitute a formal history of ASPAB, although they reveal one was written for the years 1940–52. They do not contain case files tracking an application through review to secrecy to rescission to patenting, but do tell that what may have been World War II case files were removed to the "Alexandria archives" in 1950.

For all they do not say, the ASPAB records divulge a great deal. They disclose concern as early as January 1941 that invention secrecy law could not restrain the flow of scientific and technical information to potential adversaries overseas. They acknowledge delay and error in administration of invention secrecy. They itemize Patent Office techniques for insuring wartime security. They allude more than once to potentially embarrassing administrative episodes that could jeopardize congressional action.

The ASPB records underscore problems in allocating intellectual property rights that still have not been resolved. They reveal that secrecy orders are often imposed on inventions which on their face are not patentable. They help explain corporate acceptance of invention secrecy, noting "the effect of secrecy orders in many cases is extension of the patent monopoly for what may conceivably be substantial periods beyond the seventeen-year term of the issued patent."

And Record Group 334 makes plain that only twice in the history of invention secrecy—in November 1945, on the eve of a general secrecy order rescission, and in 1976, when the National Emergencies Act was passed—have defense agencies been compelled to reassess their outstanding secrecy orders. The records partly but not fully illumine a "legal shananigan" mentioned in 1950 congressional hearings on the current Invention Secrecy Act: the assignment of patent rights by a contractor to the Government, with a reversionary clause assigning them back at a specified time.

In all, the ASPAB records explain the present by explaining the past.

PREWAR CONCERNS

Early in 1941 the Attorney General of the United States called for action to safeguard American industrial secrets for national defense purposes.[77] A document of February 19, 1941, in the ASPAB papers, headed "suggested subcommittee report or agenda" but not otherwise labeled or identified, advises that the invention secrecy statute of 1940

[77] Speech of Attorney General Robert H. Jackson before the Council of State Governments, meeting at the Mayflower Hotel, Jan. 21, 1941. Because of Jackson's illness, his speech was read by Solicitor General Francis Biddle. Typescript if Jan. 22 newspaper report of the speech. Batch V.

"may be evaded by the following actions taken before an application is filed in the United States or before a secrecy order is issued: a. Filing an application abroad. b. Sending a copy of the application or other description of the invention abroad. c. Publishing a description of the invention in the United States." It continues:

> Control of export of technical and scientific information published in a form generally available to the public might seem to be a form of indirect control of the press beyond the scope of action which could properly be recommended by this committee.
>
> Complete control of export of technical and scientific information cannot be even approached except by complete censorship.[78]

It recommends extending statutory export control authority by presidential proclamation to "any models, designs, photographs, photographic negatives, plans, specifications, documents, or other articles or materials containing descriptive or technical information of any kind (other than that appearing generally in a form available to the public)" pertaining to production, manufacture or reconstruction of prohibited or curtailed articles. It also recommends requiring that no patent application be filed in a foreign country without a license from the Commissioner of Patents.[79]

In August, the invention secrecy statute of 1940 was amended by adding license and penalty provisions. It declared:

> No person shall file or cause or authorize to be filed in any foreign country an application for patent or for the registration of a utility model, industrial design, or model in respect of any invention made in the United States, except when authorized in each case by a license obtained from the Commissioner of Patents under such rules and regulations as he shall prescribe.

It said a person who violates this provision "shall be debarred from receiving" a U.S. patent. It also said whoever knowingly violates a secrecy order by disclosing the invention or filing a patent application on it in any foreign country would face $10,000 fine or two years imprisonment, or both.[80]

On October 9, 1941, Lt. Col. Francis H. Vanderwerker of the War Department Judge Advocate General's Office wrote the secretary of ANPAB, recounting a meeting the day before he and the chief of the Navy Judge Advocate General's patent section had with the Commissioner of Patents. The meeting dealt with other matters, he wrote, but during its course.

> the Commissioner voiced as his opinion that the Army and Navy Patent Advisory Board was not recommending secrecy in as many cases as it should. He further stated that he had received a similar complaint from industry. He attributed this condition mainly to the fact that a claim against the Government might later be made, and stated that in his opinion

---

[78] Batch V.
[79] Id.
[80] Act of August 21, 1941, Public Law 77–239, 55 Stat. 657.

> such factor should not be given any weight at all. As he expressed it, if there is the slightest doubt in the mind of the expert he should recommend secrecy. In other words, if we are going to err, let it be on the side of safety.

If this condition does exist "it is particularly unfortunate," Vanderwerker wrote, "and I thoroughly agree with him that the fact that a claim might later be filed should in no wise influence the decision of the expert." He added:

> After all, this is an important and serious function with which we are charged and one erroneously issued patent may do more to injure national defense than the improvident holding of a hundred applications in secrecy.[81]

That view became official policy after America entered the war.

PATENT OFFICE SECURITY PROCEDURES

During World War II the Patent Office employed six procedures relating to security, over and above its rule of secrecy—later codified—that assured the confidentiality of all patent applications. The Patent Office War Division outlined the six in a letter of October 3, 1945, informing ANPAB that two of them were being abolished.[82]

1. Impounding—issued patents restricted as to soft copy sale, etc.
2. Super Secrecy—applications sealed without examination.
3. Special Handling—applications examined under extra secrecy precautions.
4. Blue Slip—applications forwarded to War Division at time of filing, a temporary form of *S. H.*
5. Secrery Orders—applications kept from issue or other disclosure under Public No. 700.[83]
6. Three-Year Rule—applications assigned to the Government kept from issue or abandonment under R.S. 4894.[84]

The last five could occur in any combinations on the same application, it said, "except that number 2 and 3 or 4 are mutually exclusive."

The letter announced that Impounding and Super Secrecy were being abolished. "The other procedures are used somewhat interchangeably, but all have a similar purpose," it explained. It said the same security precautions will be exercised under all procedures after November 30, 1945, "when the outstanding secrecy orders are reduced to a reasonable number" (by a general rescission order).[85]

Impounding shut off public access to issued patents. It meant discontinuing inspection of the file wrapper and sale of soft copies and, in varying degree, discontinuing inspection of examiners' copies,

---

[81] Batch R.
[82] Batch S–e.
[83] Shorthand for the 1940 invention secrecy statute, Public Law 76–700.
[84] Now 35 U.S.C. 267 (1976) : "Notwithstanding the provisions of sections 133 and 151 of this title, the Commissioner may extend the time for taking any action to three years, when an application has become the property of the United States and the head of the appropriate department or agency of the Government has certified to the Commissioner that the invention disclosed therein is important to the armament or defense of the United States."
[85] Batch S–e.

search room copies and bound volumes. A Patent Office War Division notice to ANPAB of September 12, 1945, lists six impounded patents.[86] Super Secrecy was revived in the Invention Secrecy Act of 1951:

> Upon proper showing by the head of the department or agency who caused the secrecy order to be issued that the examination of the application might jeopardize the national interest, the Commissioner shall thereupon maintain the application in a sealed condition and notify the applicant thereof.[87]

(For a Government agency, the ultimate in super invention secrecy may be to not file a patent application at all. For instance, the Signal Corps Patent Board decided in 1937 that two inventions by cryptologist William F. Friedman were so important that no patent applications should be filed. Indeed, Congress on five occasions has passed private laws awarding money to Government employees or their heirs for royalties foregone on secret cryptologic inventions—in 1935, 1937, 1956, 1958 and 1964—and in four of these cases the law is worded to acknowledge inventions on which no patent applications were ever filed. See separate section on public cryptography).

While not itself a security procedure, the wartime standard for issuance of a secrecy order was, by implication, easy to satisfy. The Patent Office signaled this in October 1945 by decreeing that "any further recommendations of secrecy should be made only after a detailed study of the application involved a decision that the disclosure would be of critical importance to any prospective enemy." [88]

APPLICATION AND INTERPRETATION, 1940–45

The assorted documents in Record Group 334 plumb the wartime workings of invention secrecy, showing how the law was applied and interpreted. As noted, it became wartime policy to issue a secrecy order rather than chance disclosing an invention having potential military utility. The Army and Navy Patent Advisory Board explained this policy in a June 1945 memorandum to the Joint Chiefs of Staff:

> While the war continued in Europe, and especially so long as Germany and Japan both had laboratory and manufacturing facilities for exploiting any disclosures which might have military value, it was clearly proper, in case of doubt, to impose a secrecy order, and this is the policy which the Board has followed up to this time.[89]

The documents contain equally explicit statements of application and interpretation, but sometimes the reasons for them are left unstated.

1. Imposing secrecy orders on obviously unpatentable inventions

In January 1944 the Assistant Commissioner of Patents responded to questions from an official of the State of California Division of

---

[86] Batch S–g. The patent numbers listed are 2,277,464; 2,300,189; 2,304,351; 2,317,026; 2,335,072; and D-127,185.
[87] Batch S–e–I.
[88] 35 U.S.C. 181 (1976).
[89] Batch C–2.

Corporations about invention secrecy remifications for State law covering the sale of securities in corporations which exploit or develop inventions under patent or for patenting. He wrote that issuance of a secrecy order "does not mean that the Government has adopted the alleged invention described in the application," and continued:

> Nor does it mean that a patent will ever be granted on such application. In fact, many such orders are issued in applications disclosing subject-matter (sic) which *prima facie* is not patentable.[90]

He gave no reason why "many such orders" were issued on obviously unpatentable inventions.

2. The Navy's view of intellectual property rights

In July 1940, three weeks after approval of Public Law 76–700, the invention secrecy statute, Navy Judge Advocate General W. B. Woodson informed its bureaus of aeronautics, ships and ordnance that the Commissioner of Patents had requested formation of a joint Army-Navy patent board. "It is contemplated," he wrote, "that the major work of the Board will be defensive in character, i.e., the prevention of the publication of inventions which, through contractual relations, have already been adopted for or incorporated in the national defense. The second function is, obviously, to comb the Patent Office for inventions which may be of interest to the various branches of the Military Services." [91]

Discussing the board's tentative procedures, Woodson broached the subject of inventor compensation and advised that "certain substantive rights in the inventor are automatically created" through issuance of a secrecy order. He wrote:

> Where the application is the property of an independent inventor or the subject matter has not previously been adopted into the national defense, the Secretary of the Navy will initiate, at the instance of the materiel bureau concerned, negotiation with the owner or inventor leading to immediate compensation, thus obviating probable future suits in the Court of Claims. In this connection, it should be noted that if the Commissioner of Patents is requested by the Secretary of War or the Secretary of the Navy to withhold the publication of an application, certain substantive rights in the inventor are automatically created, even though his invention may never be actually used; hence, recommendations for secrecy must be accompanied with an expression, implied or direct, that compensation for such secrecy will be furnished in proper cases.[92]

How often the Navy undertook to negotiate "immediate compensation" cannot be determined from the archived documents, and Woodson's instructions may subsequently have been modified, overridden by the policy of better too many secrecy orders than too few, or overtaken by events. For the record, the Navy Judge Advocate General had

[90] Batch C–3.
[91] Batch D.
[92] Id.

recommended 775 of the 7,397 secrecy orders in effect on March 25, 1944.[93]

(Few claims for compensation have been brought before defense agencies since 1945. At the subcommittee hearings, a witness from the Patent and Trademark Office testified the office does not keep track of compensation sought or paid but that he understood 29 claims had been lodged in the last 35 years.[94] At subcommittee request, ASPAB submitted a list of these administrative claims and related information, which appear in the hearing record. Further, in contradistinction to Woodson's interpretation of the 1940 law as creating certain substantive rights automatically, defense agencies apparently have chosen not to recognize such rights in the form of administrative awards for secrecy order damage claims—expressly authorized by the Invention Secrecy Act of 1951—where the invention was suppressed but not used by the Government and the Government was the sole intended market for the invention.[95])

3. Why industry cooperates in invention secrecy

No patent will issue while a secrecy order remains in effect, but holding the patent in abeyance need not curtail commercialization of the invention involved. An official of the Petroleum Administration for War wrote the chairman of the Patent Office War Division in December 1943 that his office had been considering the effect of secrecy orders "from the standpoint of the public interest, both under war conditions and during the post-war period." He continued:

> It is our understanding that when an application has been placed under the provisions of this Act, prosecution thereof continues in the normal manner, except that formal allowance is withheld during the period that the secrecy order is in effect. Unless there should be a rescission of such order after the application is in condition for allowance, it will not issue as a patent while said Act is in force. In other words, the term of the patent will not begin to run until after the war.
>
> In the meantime, of course, an applicant may be entitled to compensation for the use of his invention, either by the Government after duly making tender thereof, or by commercial operations not inconsistent with the secrecy order and any modifications of the same. Many applications under secrecy orders are being used under licenses and the owners of such applications presumably are receiving royalties for such use. Thus the effect of secrecy orders in many cases is an extension of the patent monopoly for what may conceivably be substantial periods beyond the seventeen-year term of the issued patent.
>
> This circumstance may give rise to future criticism with respect to the operation not only of Public Law No. 700, but also other laws concerning patents. For this reason it is

[93] Of the remainder, 3,310 had been recommended by ANPAB, 1,744 by the War Production Board, and 1,315 by the Office of Scientific Research and Development (Batch M).
[94] Hearings. Testimony of Assistant Commissioner for Patents Rene Tegtmeyer.
[95] See invention secrecy finding No. 8.

thought that consideration should be given as soon as possible to means for avoiding such situations.[96]

One such substantial period could be the interval between Patent Office dispatch to the applicant of what today is called a "D–10 order," or Notice of Allowability, announcing that a patent would issue but for the secrecy order, and rescission of the order. The 1940 statute authorized the Commissioner to withhold the patent grant "for such period or periods as in his opinion the national interest requires."

Further effective extension of the patent monopoly could result from combining issuance of a secrecy order with use of the "Three-Year Rule" (discussed in the chapter on Patent Office Security Procedures). Under that authority,[97] an applicant can assign his patent right to the Government, which in turn can win a three-year delay in Patent Office processing of the application by certifying—in the current language of the United States Code—"that the invention disclosed therein is important to the armament or defense of the United States." The fact of the assignment of the patent right to the Government was itself kept secret.

On May 10, 1950, a subcommittee of the House Judiciary Committee held a hearing—which was not published until 1965—on legislation which in the subsequent Congress became the Invention Secrecy Act of 1951. The first and only witness was Capt. George N. Robillard, Assistant Chief for Patents and Patent Counsel for the Navy Department of Defense. Robillard testified that if the statute of 1940, Public Law 700, were to expire, the only remaining secrecy statute would be the one permitting "the keeping under secrecy of those cases which are owned by the Government." He then declared:

> Heretofore we have resorted to a legalistic means of keeping them under secrecy when the contractor was willing. He would assign title to the United States with a reversionary assignment to him when the case was declassified. As a result by doing that we actually resort to the statute and have the Patent Office suspend action on his application because title is in the Government. However, in a sense, it is a legal shenanigan.

Robillard explained under questioning, "When we take title we suspend all action for 3 years, and nothing is done."[98]

One document in Record Group 334 alluding to the use of these procedures in combination is a letter of August 1942 from the Assistant Attorney General to the chief of the Patent Office War Division regarding an outside recommendation that a particular application be placed under secrecy order. The letter declares:

> Please be advised that pursuant to Certificate of the Acting Secretary of Commerce filed in the Patent Office with the application on February 25, 1942, the case was put under three-year rule (U.S.C. Title 35, Section 37) by Commis-

[96] Batch Y. The writer, M. R. Mandelbaum, chief of the development section in the refining division, proposed "exchange of views among the interested parties," leading to "a oasis for constructive action," to occur "at the earliest convenient time." The archived documents do not indicate whether such discussions ever took place.

[97] Originally R.S. 4894, it is now 35 U.S.C. 267 (1976).

[98] Patent Disclosure: Hearings on H.R. 6389 Before Subcommittee No. 4 of the House Committee on the Judiciary. 81st Cong., 2d sess. 17–18 (May 10, 1950) (Serial No. 24 (1965)) [hereinafter cited as "1950 Hearings"].

sioner's Order dated March 10, 1942, for the purpose of secrecy, and the assignment record is secret.

No Patent Office action on the merits of the application has as yet been rendered, and as you understand, when such action is taken, response need be made only within three years from that date.

If for any reason it is believed necessary to supplement the steps already taken by putting the case under Public Law 700, it is requested that this Department be advised so that it may be similarly guided in further cases.[99]

A second document cites actual—not prospective—use of the combination. The letter of September 1942 from the Patent Office War Division to a patent examiner in Richmond, Va., refers to "P.N. Ableson, S.N. 455,581," and explains:

This application has been placed under the provisions of Public 700 (35 U.S.C. 42) as amended in accordance with the letter of transmittal signed by W. B. Woodson, Judge Advocate General of the Navy.

In the same letter it is requested that the case also be placed under the provisions of 35 U.S.C. 37, and that the assignment be kept (sic) secret.

Thus it appears that the Navy Department considers said application extremely important and desires the utmost secrecy concerning both application and subject matter.[100]

When industrial projects deemed essential to the war effort were to generate patent applications, Government units sometimes alerted the Patent Office in advance to urge immediate secrecy. For example, the Assistant Secretary of the Navy for Air apprised the Commissioner of Patents in July 1943 that the President of United Aircraft Corporation had informed him his company planned to file patent applications shortly on 18 projects pertaining to power plant development by the Pratt & Whitney Aircraft Division. The Assistant Secretary asserted "it is clearly important to the prosecution of the war that the above applications immediately upon receipt by your office be made the subject of a secrecy order without circulation to other persons or agencies." [101]

Sometimes a Government contractor notified the Patent Office directly of changing circumstances it believed now warranted secrecy. Bell Telephone Laboratories did so in February 1943, writing the Commissioner about "Patent 2,312,514 Scheduled to Issue March 2, 1943." The letter declared:

The above-identified patent application relates to a circuit which is an alternative of something which is being incorporated in a highly secret project X–61753 under development by the Bell Telephone Laboratories, Incorporated, under the direction of the Signal Corps. This fact is being called to your attention in order that you may consider the advisability of withdrawing the application from issue and placing it under secrecy order (Public No. 700)[102]

---

[99] Batch I.
[100] Id.
[101] Batch U
[102] Batch T.

If secrecy orders issued as proposed in these aircraft engine and project X–61753 circuit examples, they may well have prolonged the period of proprietary protection for these inventions, by delaying the start of the patent clock, while the applicants did business in them with the Government.

PHASING OUT WARTIME SECRECY

World War II invention secrecy ended with a bang—a general rescission order by the Commissioner of Patents effective November 30, 1945. The Secretary of Commerce summed up wartime experience with the secrecy statute in a letter that September to the Secretary of War:

> In the administration of that law, the War Department, as well as the other defense agencies of the Government, has rendered the Commissioner valuable and necessary assistance during the present war in selecting applications for patents in which secrecy orders should be issued. Over 12,000 such orders were issued under the Act mentioned, of which approximately 8,000 are now outstanding.
>
> These orders relate to applications which have not only military significance but also commercial utility. In fact, the majority of them fall in the latter category.[103]

The Commissioner had met August 30 with defense agency representatives to determine how to release "to their owners for commercial exploitation" those suppressed applications not having purely military significance, the Secretary wrote. They unanimously agreed the Commissioner should issue a general rescinding order to take effect in 90 days, giving defense agencies time to recommend that certain patent applications be retained in secret status.[104]

The documents preserved in the National Archives record that the War Production Board authorized rescission of all its sponsored orders except those on a jet type motor and a uranium power generator.[105] The Signal Corps wrote in October it expected to recommend retaining "very few" secrecy orders but did want to review five categories of them, including "secret signaling and cryptographic devices and systems," and "electronic devices or systems which may be employed in a military role as means of countermeasures." [106] In September, the Signal Corps had notified the Patent Office War Division by serial numbers of 31 patent applications it wished kept secret and of 45 others for which "need for secrecy no longer exists." [107] The Navy Bureau of Ordnance submitted a list of 56 technical features it was "desirous of continuing in secrecy," including atomic energy, missile steering systems, underwater torpedo propulsion, radar anti-jamming measures and infrared detection equipment.[108]

---

[103] Batch C–1.
[104] Id.
[105] Batch G.
[106] Batch S–f.
[107] Batch Z (which also contains a category list of May 2, 1946, from the patents and inventions counsel in the Office of the Chief Signal Officer designating: electromagnetic wave remote control devices and systems which are applicable to guided missiles; deceptive devices, intentional signal jamming generators and systems and techniques for obtaining a desired signal in the presence of intentional jamming; and applications in the general class of "death rays," in which electrical particles or wave radiations are claimed to exert deleterious effects on human beings or machines).
[108] Batch S–d.

> the work of the War Division was substantially over and that applications of military secrecy value should be limited perhaps to the extent that the atomic bomb developments would be the only "secret" cases.[109]

Also, Lt. Col. James L. Brewrink of the Army Judge Advocate General's Office reported that discussions at the meeting with the Commissioner of Patents August 30 placed emphasis "on cases under classified contracts," and that

> it appeared that the only manner in which the inventions of an independent inventor could be located and brought within the excepted applications would be by requesting their submission at the Patent Office War Division by outlining fields of interest for such consideration.[110]

On October 19, the chief of the Patent Office War Division wrote ANPAB and the Office of Scientific Research and Development that "developments of recent months have resulted in a very definite trend to remove wartime restrictions." This was reflected at the Patent Office, he noted, by elimination of the practice of impounding patents, prospective elimination of applications held without examination, and issuance of the general rescinding order, and added:

> In view of these changes it is requested that any further recommendations of secrecy should be made only after a detailed study of the application involved and a decision that the disclosure would be of critical importance to any prospective enemy. It is also requested that recommendations for special handling or prosecution under the three year rule should be similarly considered, and that applications already under such security precautions should be systematically withdrawn from such status as fast as conditions justify.
>
> It is also requested that necessary recommendations to continue secrecy orders after November 30, 1945, be promptly forwarded to this Office so that they may be acted upon well in advance of that date. If any fields of interest have not been reported to this Office, immediate action is imperative to avoid termination of the secret status under the General Rescinding Order.[111]

After 90 days of review and preparation, the general rescinding order took effect November 30, 1945. The war's-end clearance removed 6,575 secrecy orders, leaving 799 still in force as of December 31.[112]

It was low tide for invention secrecy. Eleven months later, there were 1,140 secrecy orders.[113] In 1951, at a congressional hearing, an army witness testified the number of secrecy orders stood at "approximately 2,395," and a Patent Office witness said "very roughly there would be

---

[109] Batch O.
[110] Id.
[111] Despite the end-of-the-war optimism of the Patent Office, stated in print in the December 1945 rewrite of its security procedures, the number of secrecy orders returned only briefly to pre-Pearl Harbor levels.
[112] Information from ASPAB files in the Supplement to the History of the Army Section of the Army and Navy Patent Advisory Board, 1 April 1945 to 31 December 1945. Of the 6,575 rescinded orders, 3,829 were ANPAB-sponsored.
[113] Batch O–b.

some 3,000." [114] Secrecy orders in effect when the Invention Secrecy Act of 1951 was approved remained in effect, or by law could have, until March 1979.

THE POSTWAR YEARS, 1946–50

As times changed, so did the conduct of invention secrecy. The Army and Navy Patent Advisory Board changed its name. The Central Intelligence Agency was established by the National Security Act of 1947 and assumed certain responsibilities with respect to invention secrecy. The old system of categorical review of patent applications fell into disuse, only to be revived, and the War Department proposed a way that Government liability under the invention secrecy statute "may in many cases be cancelled" for patent applications arising from classified Government contracts.

At its meetings of September 16, 1948, ANPAB retitled itself the Armed Services Patent Advisory Board, in order that the name "might be generic to the Army, Navy and Air Force Departments." Minutes of that meeting also acknowledge that the CIA had undertaken responsibilities in connect with the 1940 invention secrecy statute, recording that:

> Mention was made of certain activities of the Central Intelligence Agency with respect to Public 700. It was agreed that efforts should be made to coordinate such activities with the Board's operations.[115]

What these "certain activities" of the CIA comprised, or whether ASPAB succeeded in having them coordinated with its own activities, is not recorded. There is no further reference or explanation in the documents of Record Group 334.

That mid-September meeting of 1948 had been called primarily to ascertain whether, "for security reasons," the Patent Office should revive its practice of screening patent applications for secrecy order potential on the basis of "certain technical fields or subjects (categories) specified by the Board." This review system "had fallen substantially into disuse" shortly after the general rescinding order of November 1945, the board's secretary said. Board members agreed

> That, instead of the three Departments furnishing the Comsioner with separate lists of the various invention categories in which their bureaus and technical services are interested, a single consolidated list of categories in behalf of the three Departments should be prepared and furnished to the Commissioner through the Board Secretary.

After discussing the security of the separate and consolidated lists, they also agreed "that these lists should be classified in order to insure proper protection." The board appointed a committee to initiate matters and agreed to meet one week later, on September 23, to draw up a tentative consolidated list "to be furnished promptly to the Patent Office as an interim list." [116]

---

[114] Patent Disclosure: Hearings on H.R. 4687 Before Subcommittee No. 3 of the House Committee on the Judiciary. 82d Cong., 1st sess. 29, 36 (Aug. 21, 1951) (Serial No. 22 (1965) [hereinafter cited as "1951 Hearings"] Patent Office files examined by staff on July 10, 1980, reveal that as of July 31, 1951, three weeks before the 1951 Hearings, there were 3,435 secrecy orders in force.

[115] Batch O–a.

[116] Id. The meeting was called because of the "urgent interest" expressed by several board members, "particularly" the Army Ordnance and Signal Corps representatives.

In June 1947, an official in the War Department Office of the Chief of Ordnance, T. E. Cosgrove, wrote the board (he later was, and may then have been, an ASPAB member) with a proposal to promote uniformity in the issuance of secrecy orders on patent applications flowing from classified Government contracts. He argued:

> When a Government Technical Service contracts with Industry for classified research and development, national security is amply protected by the contract clause which cites the Espionage Act. In view of this fact, it is thought to be advisable in certain specific cases, to withhold recommendations for the issuance of Secrecy Orders until the Patent Office has allowed the case. At that time, the desirability of recommending the issuance of a Secrecy Order can again be considered. During the period the application is pending in the Patent Office, the contractor would be required to suitably "flag" is file to indicate the relation of the case to a classified Government contract and to further specify on the "flag" that the contracting officer or his representative shall be advised of the allowance of the case in order to complete consideration of the possibility of recommending Secrecy.

Gosgrove listed four factors favoring his proposal:

> a. Government license rights are not affected.
> b. Government liability under the terms of the Secrecy Act may in many cases be cancelled.
> c. Contractors' patent interests will not be jeopardized as they would be if a disclosure was inadvertently made while the application were under a Secrecy Order.
> d. Industry may more easily follow a procedure which is uniform in all Services.[117]

The archived documents do not indicate how the board reacted to Cosgrove's proposal. However, the contemporary practice of the Army is to not request issuance of a secrecy order until the Patent Office finds the patent allowable.[118]

By 1949, new security procedures had evolved within the Patent Office. A notice distributed to all patent examiners and docket clerks, and received by ASPAB on March 10, reported that "Division 70" was charged with special security measures for:

> (a) All applications in which a Secrecy Order under 35 U.S.C. 42 is in effect.
> (b) All applications designated as "Special Handling" under instructions issued by the Commissioner.
> (c) Government owned suspended prosecution or suspended action applications.
> (d) Such other applications as may be directed by the Commissioner.

The notice also refers to a category of "5-year" applications, declaring:

> Government owned suspended prosecution or suspended action ("3-year" and "5-year") applications in custody of Di-

[117] Batch N.
[118] Information from ASPAB.

> vision 70, and which are not also subject to a secrecy order, shall be represented in the assigned division at all times by the drawings or brief cards for purposes of interference searches. Such drawings may be distributed with other nonsecurity drawings or kept separate and locked in the best means available at the discretion of the Chief of the assigned division. The application files of Government owned "3-year" and "5-year" applications, which are not also subject to a secrecy order, will be locked in the special cabinets provided in Division 70 except for such intervals as are required for performance of the examining operation.[119]

To distinguish Government-owned suspended prosecution applications "which are not also subject to a secrecy order," clearly implies that the Patent Office could again or still invoke its World War II procedure of combining the "Three-Year Rule" with issuance of a secrecy order. The "5-year" option is not further explained in the notice, but a March 15 letter from Division 70 to the ASPAB secretary twice refers to " 'suspended action' (Rule 103)" status, and reveals that such cases can "cover information entitled to a 'Secret' classification under rules of a recognized Government Department." [120] The source of "Rule 103" is not stated.

Three months later, in June 1949, ASPAB Secretary H. E. Galleher, Jr., wrote a file memorandum about a telephone call from the chairman of Division 70, James L. Brewrink, informing him

> to the effect that, where the Army Department is about to file a patent application and the classification of its subject matter is such that it is desired that all possible precautions be taken to insure its security, arrangements have been made whereby such application may be filed directly in Division 70. In this way there would be avoided any possibility of any impairment of security with respect to the case which might occur from the time it ordinarily would be filed in the Patent Office Application Division and its arrival in Division 70. Mr. Brewrink said that upon inquiry, he would be pleased to furnish any further required details with respect to this new procedure.[121]

The context of this new procedure is not discussed.

1. Peacetime Secrecy Legislation Given "Urgent" Priority

On September 23, 1949, President Truman announced that the Soviet Union had tested an atomic bomb.[122] An ASPAB memorandum three weeks later, addressed to the directors of Army, Navy and Air Force intelligence, gives first recognition in the archived documents that maintenance of invention secrecy authority was now deemed crucial to peacetime military security. Noting that existing authority

---

[119] Batch S–a.

[120] Id. The March 15 letter also says: "While no change has been made as regards to prohibiting th use of classification markings on papers filed as components of an application in the Patent Office, it is suggested that when certain applications should be treated with a higher grade of security, the need for such treatment be made known to the Patent Office."

[121] Batch K.

[122] Sweet, William. "Atomic Secrecy," Editorial Research Reports (Vol. II, No. 9), Sept. 7, 1979.

would remain in force "during the time when the United States is at war," the memorandum of October 13 explained:

> In view of the obvious importance from a military security standpoint of securing the enactment of peacetime secrecy order legislation with respect to U.S. patent applications and the inventions disclosed therein, proposed legislation covering this subject now has an "Urgent" priority on the Department of Defense legislative program and has been presented to the 81st Congress by S. 2557. A companion bill is about to be introduced in the House.[123]

It then warned that 'what on their face appear to be abuses" of existing law might thwart enactment:

> Thus, there is present the possibility of jeopardizing the enactment of such legislation should allegations be made to Congress, by persons opposing the legislation, of what on their face appear to be abuses of the present Secrecy Order Act, above mentioned, by maintaining in secrecy U.S. patent applications where corresponding foreign patents have issued and been given such publication as substantially to impair the security of the disclosures of the corresponding U.S. patent applications.[124]

The six-page memorandum told the intelligence directors that ASPAB's principal function was to advise the Commissioner of Patents on imposition and rescission of secrecy orders, and that it wished to pose this question:

> Under present security policies and directives, should [ASPAB] recommend to the Commissioner of Patents, with respect to each patent application in which a secrecy order . . . is in force, that such order be rescinded where it has come to the Board's attention that a foreign patent (or patents) corresponding to such U.S. application has issued, and particularly where the foreign patent (or patents) has been given such publication as substantially to impair the security of the disclosure of the U.S. application?

It said their instructions were "urgently needed" in view of the interest of the British Commissioner of Patents in this question and given "certain pending petitions" for rescission, including "Petition No. 532 (dated 12 June 1949) relating to U.S. Patent Application, Serial No. 503,523, by William A. S. Butement et al., and Petition No. 533 (dated 28 June 1949) relating to U.S. Patent Application, Serial No. 760,423, by Edgar W. Brandt." The board's enclosures dealing with these two petitions (not found in Record Group 334) bared "a divergence of views" on whether they should be granted. The memorandum continued:

> Although most of the members recommend granting of the petitions to rescind the secrecy orders in view of the issuance of certain corresponding foreign patents, the Army Ordnance

---

[123] Batch A–11.
[124] Id.

> Department and the Air Force Department Members recommend denial of Petition No. 532, and the Army Ordnance Department Member has made a similar recommendation with respect to Petition No. 533.

It asked for "closely coordinated" responses from the intelligence agencies, leading to a "uniform ruling" that could be adopted as board policy.[125]

2. 1950: An Upsurge Of Secrecy

By mid-1950, the ASPAB secretariat found itself overwhelmed by a much higher volume of applications and petitions for secrecy order issuance, rescission and modification. The June 28 meeting took up "the urgent need of clerical assistance" and blamed the Navy for most of the upsurge of secrecy. Minutes of the meeting record that an Army major and the ASPAB secretary, H. E. Galleher, Jr.,

> pointed out that the Judge Advocate General's Office, Department of the Army, has furnished the secretary for the Board practically ever since its inception and substantially all other persons who assisted the secretary in the Board work; that this work, in addition to the Secretary and the stenographer presently doing the work, now requires the *additional* full-time help which would be provided by a clerk-typist and which JAGO is unable to provide; that the vast majority of the cases in secrecy have been sponsored for secrecy by the Navy; and that it appears only reasonable to ask that the required help be furnished by the Navy. Mr. Galleher presented Board records to substantiate the foregoing.[126]

These assertions led to a "prolonged general discussion" of whether the need for help was real, how such help could be obtained and of possible steps to obviate the need by simplifying board operations in the circulation and signing of papers. A motion was made to authorize the board secretary to recommend issuance of secrecy orders "on behalf of the Board, based upon the recommendation of a single Board Member, thereby eliminating circulation of the recommendation papers among any other Board Members," then modified to the recommendation of all the board members from any one uniformed service, and then withdrawn to permit further study.[127]

Record Group 334 does not contain summaries of overall secrecy order activity as of given 1950 dates. However, it does contain two lists, which may or may not be representative, of changes in Navy-sponsored patent applications in secrecy as of November 1. Together they show 73 new secrecy orders, four "returned to secrecy" and nine orders rescinded.[128]

Under date of September 7, ASPAB sent the Commissioner of Patents a new "Armed Services Consolidated List of Classified Subject Matter," or invention secrecy field-of-interest list, to replace the

---

[125] Id. (ASPAB files disclose that the secrecy order on the application by Butement, Edward Samuel Shire and Amherst Felix Home Thomson—which has been "returned to secrecy" on June 29, 1947—was not rescinded until Jan. 29, 1959. Patent Office files show that the application by Brandt, of Geneva, Switzerland, resulted in Pat. No. 2,613,605, issued Oct. 14, 1952.)

[126] Batch A–10.

[127] Id.

[128] Batch M.

one it had filed on October 7, 1948. The 14-page list was set forth in 19 subject groups ("explosives and inflammables"; "navigation equipment"; "propulsion means"; and so on), keyed by abbreviation to the interested service unit. In the Army, these were Ordnance, Signal Corps, Chemical Corps, Corps of Engineers and the Surgeon General, and in the Navy, the bureaus of ordnance, aeronautics and ships. In December, ASPAB requested some changes in the list, particularly in items under Group IX ("Concealment, Anti-concealment, Inteference or Anti-interference"). The principal revision read:

> Item 6, change to read, "Signalling or communication, secret means or methods for (*Ships*), (*SC* Signaling and communication, secret, means and methods for, and cryptanalytics: specifically, cryptography (manual, typewriter, and teletypewriter techniques, and apparatuses), enciphered telephony and other speech systems, enciphered facsimile and television equipments, secret inks, secret microphotography, flash signaling and other types of concealed electrical communications, and all means and measures, cryptologic and otherwise, for deriving the essential information from enemy communications of the natures indicated." [129]

This list, classified "Secret," lasted at least until March 1953, when ASPAB launched another review for possible changes.[130]

In the postwar years, invention secrecy was not confined to atomic bomb developments as H. H. Jacobs of the Patent Office War Division had expected. From July through December 1945, the Patent Office had rescinded 8,764 secrecy orders in its World War II closeout,[131] but the number in force grew in 1946 and, as shown by interpolation, each year thereafter. Old secrecy practices were revived and new ones introduced. And in 1951, Congress granted authority for invention secrecy in peacetime.

THE DAWN OF PEACETIME INVENTION SECRECY

In the spring of 1951, the Armed Services Patent Advisory Board was again—or still—considering whether signatures of a board majority were necessary to place a patent application under secrecy order. At its May 23 meeting the board reviewed use of the "immediate action letter" for triggering a secrecy order, determining that the increasing use of such letters by board members "was brought about by necessity and that a misuse was not present." Minutes of the meeting suggest the "immediate action letter" was an individual device:

> The Board then considered whether or not it was necessary in view of the use of the immediate action letter for a majority of the board to sign the circulation papers for placing an application under an order of secrecy. It was determined that the papers should be circulated throughout the board since more than one technical service may have an interest in the cases sponsored by the other members, and in all cases the remaining signatures other than the sponsors are not placed thereon as

[129] Batch A–8.
[130] Batch A–3.
[131] Handwritten note in Patent and Trademark Office Special Laws Administration Group files (received July 1, 1980).

> a matter of form, as was previously believed to be the case. It was therefore the conclusion of the Board that (a) placing an application under an order of secrecy was a Board action and the records should so indicate and (b) confirmation of the immediate action letter by the Board was also a necessity.

The board then "reiterated the policy that the immediate action letter should be used only in cases of emergency," such being "to preserve the security of classified information contained in such applications for Letters Patent." [132]

Much of the May 23 meeting was devoted to international aspects of invention secrecy:

a. The board discussed receiving requests from the British Joint Services Mission to invoke "paragraph 4c(1) of the Combined Chiefs of Staff Agreement," which "in substance provides that where information has been disclosed to military representatives under an interchange agreement, each country when requested by the other country shall use its best endeavors to have maintained in secrecy any patent application filed in the recipient country." The minutes relate:

> In the past it has been the policy of the Board to confirm the disclosure of the information to the United States military representatives. This practice has resulted in the expenditure of much time by the interested technical service and is believed by the Board to be a precaution without the spirit of the Agreement. Therefore, in the future, it was decided that the Board will place all requests from the British Joint Services Mission, which state that a disclosure has been made to a United States military representative, under an order of secrecy without confirming the disclosure.[133]

b. On determining the foreign countries "which the Board would consider for foreign filing," not further explained, the ASPAB secretary reported that:

> responses to the letter submitted to G–2 for information to be obtained through the United States Military Attaches were being received. That, to date, however, several responses had not been received, and accordingly, no further action could be taken with respect thereto at this time.[134]

c. It also debated the handling of petitions to rescind that indicate publication may have occurred—"a violation of the secrecy order which in many instances compromises the subject matter"—and decided that where the board "is clearly of the opinion that the subject matter had been compromised that the opinion of one member would not be sufficient, as in the past, to prohibit the modification or rescission of the secrecy order." It then took up "the Butement case," one of two examples it had cited in appealing to intelligence chiefs in October 1949 for instructions that were "urgently needed." (At that time, the Army Ordnance and Air Force members of ASPAB opposed

---

[132] Batch A–7.
[133] Id.
[134] Id.

Petition No. 532 to rescind the Butement secrecy order. See note 65.) Minutes of the meeting record that—

> the facts of this case were presented to the Board and in view of the 8 to 1 decision previously rendered on the circulation papers, the Board voted for rescission. The Board, however, concluded that the Secretary should resubmit the case to the Ordnance Department with a summary of its history, together with notice of the proposed action to be taken by the Board (recommendation of rescission) in the near future unless additional reasons are submitted by the Ordnance Department to change the present view of the Board.[135]

(Ordnance stuck to its guns. Minutes of the November 26 meeting report that when ASPAB requested "more cogent reasons for maintaining the Butement case under an order of secrecy" and advised it was contemplating rescission of the order, the Ordnance reply "merely reiterated its previous position and requested that G–2 be advised of the contemplated action of the Board since the responsibility for any repercussions that might result from the publication of the information contained therein will fall upon that agency directing such action.[136] Final disposition of the Butement case is not recorded in the archived documents.)

Meanwhile, Congress was considering legislation to make invention secrecy permanent. A subcommittee of the House Judiciary Committee held a 65-minute hearing May 10, 1950, on H.R. 6389, a bill "to amend the act relating to preventing the publication of inventions in the national interest, and for other purposes" (see note 38a). The lone witness, who was Navy patent counsel, declared in his prepared statement:

> The Department of Defense is convinced that the granting of the proposed authority (is) of the utmost importance. If it is not granted, a large section of classified material, which should be withheld from publication, will be compromised immediately upon the official termination of the war.[137]

He explained why industry wanted an amendment, which he said the Defense Department considered "acceptable," to permit filing of a patent application which could then be sealed and withheld from further processing:

> The Armed Services Procurement Regulations provide that the armed services may forbid the filing of a patent application when it discloses matter which has been classified as secret or higher. Government contractors feel that this restriction deprives them of a property right inasmuch as they cannot obtain a filing date on a patent application and if they could file at a later date when the classification has been reduced they might stand to lose substantial rights. This right has been exercised by the armed services in a

---

[135] Id.
[136] Batch A–5.
[137] Testimony of Capt. George N. Robillard in 1950 Hearings, p. 18. Robillard said his statement had not been cleared by the Bureau of the Budget, but that except for discussion of proposed amendments it was in substance the same as the statement submitted with respect to H.R. 4420 in the 80th Congress, which had been cleared.

> limited number of cases. It is believed that if the Commissioner of Patents had authority to seal an application there would be little or no necessity for exercising the right to prevent filing.[138]

The following year, in the 1st Session of the 82d Congress, the same subcommittee (though renumbered) of the House Judiciary Committee held a hearing August 21 on the bill H.R. 4687, which became the Invention Secrecy Act of 1951. (This hearing, like the 1950 hearings, was not published until 1965. See note 54.) H.R. 4687 was introduced July 3, 1951, by Representative Emanuel Celler, chairman of the Judiciary Committee, as "The Patent Secrecy Act of 1951." The August 21 hearing took up an amended version which was published as a committee print dated August 21.[139]

The first witness, Dr. M. O. Hayes, who was Office of Naval Research patent counsel, had been chairman of the Navy section of the Army and Navy Patent Advisory Board from 1940 until 1946. He testified:

> As you know, we have been trying since about 1946 to get some such legislation as this passed, and in view of the possible termination of the war with Germany and a treaty of peace with Japan, it is of the utmost importance that the inventions disclosed in patent applications should be given the protection afforded by the legislation proposed in this bill.[140]

Asked about the bill's provision limiting the duration of peacetime secrecy orders to renewable periods of one year, Dr. Hayes drew upon ANPAB's experience:

> That points out that it requires an act of the agencies to make that affirmative determination at the end of each year. We tried that when we started on the (ANPAB). We said we are going to review these so that we do not keep these under a secret order any longer than a year. We found that it was impossible with the staff that we had. We could not review them. We did not have staff enough to get the applications examined in the first place for the issuance of a secrecy order, and it is going to mean, necessarily, an increase in the staff available to the defense departments for reexamining these cases each year. You see, if you have 3,000 cases under secrecy orders that means you have to examine 250 of those cases a month, which is an average of 10 a day if you call 25 working days a working month, and it was our experience that it was extremely difficult for the engineers and technical men who had to examine these applications in the first place to decide whether a secrecy order should be issued as they were overloaded with their engineering and technical duties in the bureaus.

He recommended striking the requirement that they be renewed annually.[141]

---

[138] Id. at 14.

[139] One change in the committee print was the addition of the provision, "An order in effect, or issued, during a national emergency declared by the President shall remain in effect for the duration of the national emergency and 6 months thereafter." 1951 Hearings, p. 5.

[140] Id. at 7.

[141] Id. at 8.

Another witness, the chairman of the laws and rules committee of the American Patent Law Association, disagreed with Dr. Hayes, saying:

> . . . we believe quite strongly that there should be a very definite limitation on the duration of the secrecy order. The experience during the last war, of course, when a large number of applications were under secrecy, and when the number of personnel was short prevented the reexamination of many cases which should have been reexamined long before the secrecy orders were lifted, and since this 1-year limitation applies only in time of peace, in normal peacetime, and the inventors should be permitted to exploit their inventions to the best of their ability without restriction, we believe that the 1-year limitation should remain, or if the committee felt that was a little too short at least that there should be a very definite limitation on the duration of the secrecy order in peacetime, requiring a reexamination before it is reimposed.[142]

The APLA witness noted the tradition that "applications are held in secret and not disclosed to anyone outside of the Patent Office while they are pending," but that under the bill "there is a disclosure which is contrary to the usual rule of secrecy in the Patent Office and, therefore, it is deemed proper to have a record of who outside of the Patent Office has seen the application for what it is worth." Subcommittee Member Edwin E. Willis then remarked:

> That is a rather odd procedure, is it not? Here we are preserving the secrecy of a patent which could be dangerously used against us and guarding the secrecy, and one of the procedures to effectuate the bill is to violate the normal rule of secrecy so that more people see it than otherwise would see it.

The witness responded, "You have to disclose it to an expert in a Defense agency who determines whether or not it is important to the national defense.[143]

When the witness observed that "the right to impose a secrecy order in peacetime is a drastic thing," a three-way discussion ensued with Mr. Willis and staff over the duration of secrecy orders and the need to reevaluate them. Subcommittee Counsel L. James Harris stated:

> May I say on this point that on page 4 of the committee print we inserted a provision to the effect that during a national emergency declared by the President these orders do not have to be reexamined. What we are talking about now is the case of actual peace, and since at the present time we are living in this national emergency for some time, this provision can be reexamined at some later date. It would not affect us for quite some time to come.

Representative Robert L. Ramsey added, "Under the conditions the gentleman just quoted it may be necessary to keep the secrecy of patents for years." Witness Rose concurred, saying "It is quite possible; yes, sir." [144]

---

[142] Testimony of Paul A. Rose in 1951 Hearings, p. 15.
[143] Id. at 14.
[144] Id. at 16. President Truman had proclaimed a national emergency on Dec. 16, 1950. (64 Stat. A454).

Discussion continued on the nature of inventions that could justify a peacetime secrecy order. Mr. Willis of Louisiana observed that "we all have in mind when we talk about secrecy and national defense, some weapon or some new invention almost along the line of atomic energy, and none of us would oppose that kind of legislation on that question, but we must remember that this bill goes much farther than that. For instance, during the last war such things as paint were held to be necessary for the national defense." He explicated:

> I remember a new paint was invented that made it unnecessary for ships to come to port except every year or 18 months instead of once every 6 months. This bill would apply to paints as well as secrets along the line that we usually have in mind. I am thinking of a borderline case where you are vesting in someone the power to sit on a patent for a long time. I am for the bill, but I am trying to be critical in order to see if we cannot work out something that will be satisfactory to all.

Counsel asked, "Could some reasonable time be used instead of 1 year, or can we break it down into categories?" The witness said he did not believe so, adding:

> We think it is sufficient if the important cases could be checked so as to come up automatically, and within the limits of the personnel situation the others should be reexamined. If we need more personnel I think the protection of the inventors would warrant adding a few additional personnel to take care of the additional burden.[145]

In his prepared statement, the American Patent Law Association witness underscored the need for invention secrecy authority in peacetime. He contended:

> In view of the importance of technological developments in modern warfare and the necessity of maintaining a superior military position at all times under conditions as they exist in the world today, it must be recognized that legislation of this character is necessary, regardless of the technical existence or nonexistence of a state of war. Accordingly the American Patent Law Association interposes no objection to the bill in principle.[146]

Another witness, the patent adviser in the Munitions Board, Department of Defense, made the same point by referring to a question Mr. Willis had posed:

> He asked what would happen if the war were over and all these applications were released to the public? That has been rather well answered, except this phase of it; that, in addition to the present applications that are under secrecy, all the new inventions from then on would be flowing to foreign countries. I think that is very important, and that we should not overlook it. That is the importance of a peacetime secrecy

[145] Id. at 16–17.
[146] Id., p. 26.

act; the inventions with which you fight the next war are made during peacetime before the war.[147]

In a brief appearance, Roland A. Anderson, chief of the Patent Branch, Atomic Energy Commission, asked about the distinction in the bill between inventions in which the Government "has a property interest" and those in which it does not. "I do not know that property interest is clearly defined," Anderson said. "To me it certainly is not in this bill. I am not so sure there is a clear definition, at least, in my mind, as to what is meant by the distinction between the two groups of cases in section 1." This exchange with subcommittee counsel followed:

> Mr. HARRIS. We are referring to a property interest in the bill which, in the main, will be present in inventions made by Government employees, or Government contractors. That is the distinction, and that will be stated in the report.
>
> Mr. ANDERSON. Does that mean if the Government merely acquires an interest, a nonexclusive right under its contract, that that is called a property interest? That was the kind of thing we tried to find out, what is the intention; whether it was necessary to have complete title, or anything less than complete title, which might be called a nonexclusive right, which sometimes has been the case of Government-owned property, and whether that would be an interest that would be intended here.
>
> Mr. HARRIS. That will be explained in the report.[148]

The Judiciary Committee's report on the bill, submitted September 24, did not use Anderson's example of the Government acquiring "a nonexclusive right under its contract" in explaining what the phrase "property interest" was intended to include. First it noted that the bill was making a distinction based on the presence or absence of a property interest that was not made in the invention secrecy status of 1940:

> An important difference between this bill and Public Law 700 is that this bill sets up two groups of patent applications based upon whether the Government has a property interest in the invention. If the Government has a property interest, issuance of a secrecy order requires only a recommendation to the Commissioner of Patents by the head of the department or agency involved. The phrase "property interest" is intended to include the ownership of all rights in the invention or to a lesser interest therein such as, for example, cases where the foreign rights are retained by the inventor, or where the Government is entitled only to the interest of one or more joint inventors, and not to the interest of all the joint inventors. This group will consist in the main of inventions made by Government employees or Government contractors. In the other group, the Secretary of Commerce informs the heads of the defense agencies of patient applications whose disclosure might be detrimental to the national security. This group consists for the most part of inventions made by persons not in contact with the Government. It is necessary for the Secretary

[147] Testimony of Ray Harris in 1951 Hearings, pp. 38–39.
[148] Id., p. 34. (Note: Mr. Anderson is incorrectly identified in the 1951 Hearings as "Ronald Anderson.")

> of Commerce to call the attention of the defense agency to the particular application, since they would otherwise have no knowledge of such application. The opinion of the defense agency concerned is controlling and the order that the invention be kept secret will be made pursuant thereto. * * * [149]

In its report, the committee characterized the amended version of H.R. 4687 it was recommending as "largely H.R. 6389 (of the previous Congress) with minor amendments resulting from the suggestions of industry representatives acceptable to the Department of Defense which are intended to make the bill more equitable, and amendments relating to form." [150] The report singled out other changes the bill would make in existing law:

Secrecy Orders: The period of secrecy is 1 year, or for the duration of a national emergency declared by the President and 6 months thereafter, or for the duration of hostilities and 1 year following cessation of hostilities. Under Public Law 700, a secrecy order remains in force until rescinded.

Appeal Procedure: Public Law 700 makes no provision for appeal from the secrecy order. This bill gives the owner of a patent application placed under a secrecy order the right to appeal from the order to the Secretary of Commerce. This amendment is for the protection of persons affected by the secrecy order.[151]

Compensation: Section 3 of the bill differs from Public Law 700 with respect to compensation payable to the owner of an application under a secrecy order. Like Public Law 700, however, it provides for compensation for damages caused by the order of secrecy or for governmental use. Section 3 prescribes a 6-year statute of limitations. It does not require tender of the invention to the Government precedent to recovery of compensation, nor does it defer presentation of a claim for compensation until after a patent issues on the application. It authorizes the head of a department who caused the secrecy order to be issued to make full settlement or, if that cannot be effected, a settlement not exceeding 75 percent of a just compensation. The owner who fails to secure a satisfactory award or who does not apply for compensation may bring suit in the Court of Claims.

Foreign Filing: The bill prohibits filing a foreign patent application prior to 6 months after filing a U.S. application, unless a license is first obtained from the Secretary of Commerce. This is to prevent filing abroad before the Secretary of Commerce has had an opportunity to examine the application. Under Public Law 700, a foreign filing was not permitted unless authorized by the Government.[152]

The House report espoused a need for invention secrecy in times of peace as in times of war, declaring

> The necessity for enacting the eexisting law in permanent form is considered extremely important by the Department of Defense. Moreover, there apepars to be general approval of the purpose of the bill. Inventions useful in war are made and developed during times of peace and it is important to

---

[149] H. Rept. No. 1028. 82d Cong., 1st sess. 4–5 (Sept. 24, 1951).
[150] Id. at 3.
[151] As introduced, H.R. 4687 provided a right of appeal to the agency requesting the order, "under such rules as may be prescribed by the President."
[152] These changes paraphrased from pages 5 and 6 of the report.

> prevent knowledge of such inventions being disclosed during times of peace as well as times of war.[153]

Earlier, it argued that the imminence of a congressional declaration of the end of the war with Germany and the signing of the Japanese Peace Treaty "places this bill in the class of urgent legislation." [154]

Finally, the report said, "Basically, the bill does not make changes in existing law with respect to its administration," and explained:

> Since the passage of Public Law 700, it has been administered in close cooperation with the defense agencies. The examiners of the Patent Office submit applications to the Patent Office Defense Division to determine whether they disclose inventions important to defense, and the Secretary of Defense has appointed a Patent Advisory Board to consult with the Division and assist in the determination of the applications which should be maintained in secrecy. If enacted, the Defense Department would continue to have access to pending patent applications selected by the Secretary of Commerce which in his discretion would be detrimental to the national security if disclosed.[155]

The bill was placed on the consent calendar and passed the House without debate on October 4, 1951. In the Senate, the Committee on the Judiciary reported favorably on H.R. 4687, without amendment, on October 16 (Senate Report No. 1001 said it "repeats in substance the House Report"). On October 20, the Senate agreed to two amendments to the bill (one of them gave claimants the right to sue either in the Court of Claims or in Federal district court) and passed it, without taking a recorded vote.

In January 1952 the House agreed to the Senate amendments. President Truman signed the bill on February 1, and the Invention Secrecy Act of 1951 became Public Law 82–256. Codification followed a few months later.[156]

The Armed Services Patent Advisory Board met promptly, on February 6, to consider the effect of the new law. Minutes show the board believed it would now need to be chartered by the Secrtary of Defense but decided it "could continue to operate on an interim basis as long as the Patent Office would recognize (its) actions . . ." The board also considered the provision of the new law "pertaining to the national emergency to determine whether or not the applications placed in secrecy would have to be reviewed within one year." The minutes recite that an ASPAB member, Lt. Col. Willard J. Hodges, Jr., chief of the patent division in the office of the Army's Judge Advocate General, asked while testifying at the 1951 Hearings whether the provision in the pending legislation that a secrecy order will remain in effect for the duration of a national emergency plus six months would apply to the national emergency that had been in effect since December 1950. He was told that "the presently declared national emergency would apply." [157]

---

[153] Id. at 6.
[154] Id. at 4.
[155] Id. at 7.
[156] See text accompanying notes 5–7.
[157] Batch A–5.

Sixteen months later, the nature of ASPAB's charter had not been resolved. The board met June 9, 1953, to discuss changes in its proposed charter and make recommendations to the Secretary of Defense. The minutes show that the charter originally submitted was questioned on grounds that the Invention Secrecy Act, now codified in sections 181–188 of title 35 of the United States Code, vested authority in the Secretary of Defense, not in the secretaries of the military departments. Army 1st Lt. Donald Voss disagreed, basing it on the power conferred when the Government has a property interest in an invention:

> Lt. Voss countered with the statement that the Secretaries of the Military Departments do have some authority vested in them under the provisions of Title 35 U.S.C. Section 181, that is, where the Military Departments have a property interest in an invention, the Commissioner upon being notified that the disclosure would be detrimental to national security shall order the invention to be kept secret.

The board then concluded that

> a delegation of authority from the Secretary of Defense to the Secretaries of the Military Departments would be obtained and that the Secretaries of the Military Departments, in turn, would redelegate and delegate, as appropriate, the authority to the Army Section, the Navy Section and the Air Force Section of the Board; this to be accomplished right in the charter for the Armed Services Patent Advisory Board.[158]

The archived documents essentially conclude their account of ASPAB at that point. Record Group 334 contains a few documents to 1956 and three dated 1961, but as an explanatory set it stops in mid-1953. The history of invention secrecy since then must be found elsewhere.

According to Patent Office records, the number of secrecy orders climbed to 6,149 by December 31, 1958, dropped to 4,503 at the end of 1963, and rose to 5,092 at the end of 1967. On January 1, 1971, there were 5,006 secrecy orders in force. The number declined to 4,887 at the beginning of 1973, to 4,145 at the beginning of 1976, and to 4,109 at the outset of 1978.

II. PUBLIC CRYPTOGRAPHY

A. Findings

1. The private sector is involved in a high-stakes development process involving cryptographic research. The principal issue, from the vantage point of the National Security Agency, is the extent to which "national security concerns" should influence cryptographic research, commercial development, publication or discussion outside the governmental arena. In this committee's view, the principal issue is the security classification of private ideas.

The NSA declares that its first area of concern relates to the U.S. Government's ability to gather foreign intelligence from the commu-

[158] Batch A–1.

nications of foreign governments or other foreign parties. As information about cryptography proliferates, the NSA contends, our potential sources of intelligence are reduced by making foreign governments or parties aware that their cryptographic systems are vulnerable to interception and solution, or by encouraging them to develop or adopt more sophisticated systems that are much more difficult for the United States to break.

Its second concern is that substantial work in the cryptographic and cryptanalytic fields, together with widespread dissemination of resulting discoveries, could lead to the publication of cryptographic principles or applications similar to those used by the U.S. Government. This happenstance, the NSA argues, might enable foreign powers to mount a more successful cryptanalytic attack on U.S. telecommunications.

The NSA, established 28 years ago by a presidential memorandum that has never been made public, is not the only agency involved in this development process. The National Telecommunications and Information Administration of the Department of Commerce and the independent National Science Foundation are playing or will play key roles.

This high-stakes development process seems to be taking three separate but concurrent forms:

(1) The NSA has engaged the academic and industrial communities in a dialogue over public—i.e. nongovernmental—cryptography. In the academic forum, the dialogue concerns the necessity, feasibility and desirability of some form of voluntary prior restraint on publication of research results and other information relating to cryptology.

(2) The NTIA has been charged with proposing a national policy—balancing the public interest in cryptographic research with other national interests—to a special Subcommittee on Telecommunications Protection chaired by the director, Office of Science and Technology Policy. (By presidential directive, the subcommittee exercises telecommunications policy responsibility for the National Security Council Special Coordination Committee.)

(3) The NSA has been trying to assume responsibility for much of the unclassified research relating to crytography that has been or would be sponsored by the National Science Foundation.

Based on a nine-month subcommittee study of the ability of the Government to classify, restrict or assert ownership rights over privately generated data, the committee finds that efforts by the intelligence community to restrict public cryptography pose enormous questions of constitutional validity.

The committee also finds that Congress has not involved itself in this development process. If the Congress waits, it may discover that, by regulation or by agreement, cryptographic information has acquired the "born classified" status of atomic energy Restricted Data.

2. One of the unknowns in the public crytography equation is the "Exceptional Cases" provision of President Carter's Executive Order 12065 on National Security Information, which reads:

> When an employee or contractor of an agency that does not have original classification authority originates information believed to require classification, the information shall be pro-

> tected in the manner prescribed by this Order and implementing directives. The information shall be transmitted promptly under appropriate safeguards to the agency which has appropriate subject matter interest and classification authority. That agency shall decide within 30 days whether to classify that information. If it is not clear which agency should get the information, it shall be sent to the Director of the Information Security Oversight Office established in Section 5–2 for a determination.

The President's order took effect December 1, 1978. As of September 10, 1980, the oversight office (ISOO) reports having had no action under the "Exceptional Cases" provision. However, it may have been seen as a bargaining chip in relations between the National Security Agency and the National Science Foundation.

In the past the NSF had authority for original classification of information as "Secret" or "Confidential." However, the Carter order stripped the NSF and 10 other agencies of original classification authority while providing them with an "Exceptional Cases" outlet. Classification questions generally do not arise with respect to research results under NSF grants, notes an August 18, 1980, memorandum to the NSF Acting Director from his legal department. It continues:

> However, where there is good reason to believe results may be sensitive, NSF may have a responsibility to send the results to the appropriate subject matter agency for classification review. Information is not "classified" until it has been formally determined to be so by the responsible official.

The "Exceptional Cases" provision applies to "an employee or contractor" who originates information believed to require classification, while the NSF security regulations (45 CFR 601) revised and republished in January 1980 pursuant to the Carter order provide, "In any instance where a Foundation employee develops information that appears to warrant classification . . . ."

The NSF formulation is a narrow reading of the Executive Order, assuming that the word "develops" is not meant to include information produced by a contractor under the tutelage of an NSF employee. The Carter Executive order also provides (section 1–602), "Basic scientific research information not clearly related to the national security may not be classified." Taken together, they appear to mean there is virtually no expectation that an NSF contractor doing basic scientific research could generate information so clearly related to the national security that NSF would find itself obliged to forward the information to another agency for a second opinion.

On this analysis, the NSF would not send research results in public cryptography to the NSA to determine whether the information should be classified. The NSF does send to NSA—for information purposes and technical comment in the nature of peer review—copies of grant proposals received by the Mathematical and Computer Sciences Division which bear explicitly on cryptology.

The NSF encourages—and sometimes requires—publication of research results, so whatever the NSA may not know about NSF's unclassified research support it generally will find out on publication. At the hearings, Admiral B. R. Inman, NSA Director, testified, "We are

aware of an awful lot of the activity that goes on through cooperation from across the academic community."

3. The committee commends the National Security Agency for reducing its portfolio of invention secrecy orders. At the hearings, NSA Director Inman testified that the agency began a review of its portfolio before the September 1978 effective date of the National Emergencies Act (which would result six months later in termination of all secrecy orders more than one year old unless they were formally renewed), that it rescinded 62 secrecy orders in one recent year alone, and that it now has seven secrecy orders in force, of which six cover cryptologic inventions made more than 40 years ago.

Two widely publicized NSA-sponsored secrecy orders in 1978 spotlighted "not a faulty law but inadequate Government attention to its application," Admiral Inman testified. He explained that the agency has now instituted procedures in which "a board of the most senior experienced employees of the agency must concur if one seeks to impose secrecy on any patent application."

The committee is gratified to learn of the change. The Invention Secrecy Act provides that the Commissioner of Patents and Trademarks shall order an invention be kept secret on being notified of the opinion of an agency head that its disclosure would be detrimental to the national security. The responsibility is placed on an agency's chief officer. An unjustified secrecy order—like the one the NSA had placed on Prof. George Davida—cannot be excused as a well-meaning mid-level blunder.

4. In the conduct of invention secrecy, the Patent and Trademark Office gives the National Security Agency too much the benefit of the doubt. At the subcommittee hearings, the following exchange took place between Congressman Weiss and Assistant Commissioner for Patents Rene D. Tegtmeyer:

> Mr. WEISS. Suppose there is a conflict between two agencies concerning whether or not a secrecy order should issue. Suppose the invention has been financed through a National Science Foundation grant and the NSF regulations require that all such projects must publish their results. The NSA, however, says that a secrecy order should be imposed. Who decides that matter, the Patent Office or the National Security Agency?
>
> Mr. TEGTMEYER. If we get a request from the National Security Agency that a secrecy order be imposed, we will impose it, although as I mentioned before if we see any reason that is obvious to us to question whether a secrecy order should be imposed, we do raise that question.

The Committee is unclear whether this means that an invention resulting from NSF-supported research in cryptography would always be brought to the NSA's attention (which is what happened in Prof. Davida's case).

The Invention Secrecy Act makes a distinction between two groups of patent applications. The act separates applications into two groups: Those in which a Government agency has a property interest, and those in which no agency does. In the first case, it is the head "of the interested Government agency" who may request a secrecy order.

In the second case, the Commissioner refers the application for defense agency review if he thinks its disclosure might be detrimental to national security, and if the head of that agency believes disclosure would be detrimental, he may request a secrecy order.

In the first group, the statutory word "interested" pertains to the agency having a "property interest" in the invention. In the second group, where no agency has a property interest, the application will be reviewed by defense agencies interested in the subject matter of the invention.

The military services rely on this distinction to file classified patent applications and request secrecy orders on inventions in whch they have a property interest. Indeed, they seized upon it at the first meeting of the Armed Services Patent Advisory Board after the Invention Secrecy Act became law in 1952 to demonstrate that it vested authority in the individual service secretaries as well as in the Secretary of Defense. Further, when the NSF or any other agency having a property interest in a cryptographic invention eschews a secrecy order on it, the Commissioner is given firsthand evidence not to believe that disclosure of the invention might be detrimental to national security.

However, in case where one agency has funded the invention, the Patent and Trademark Office has not established guidelines either in practice or policy as to what circulation, if any, the application will receive among the defense agencies and under what conditions, given the distinction spelled out in the Invention Secrecy Act. Where a dispute results among two or more agencies over a secrecy order, neither has the Patent Office established what mechanism will be used to resolve the dispute and who under the statutory scheme ultimately will make the decision regarding the orders' imposition.

On April 20, 1977, two National Security Agency officials, Cecil C. Corry and David G. Boak, visited officials of the National Science Foundation's Division of Mathematical and Computer Sciences to express concern about the latter's support of cryptographic research. In the meeting the NSA officials—

> Suggested that a presidential directive gave them "control" over all cryptographic word and that NSF was operating outside that directive. The NSF officials replied that they had checked into that matter nearly two years earlier and been told there was no such directive involving research. The NSA officials remarked offhand that "they would have to get a law passed."
>
> Complained about a new journal of mathematical cryptology, called Cryptologia, which supposedly was funded by NSF grant "IG 3454." The NSF officials said they had nothing to do with the publication.

At that meeting, the NSA representatives asked that the NSF Division keep them informed of proposed research in the cryptology area. The NSF officials agreed to use NSA personnel as reviewers of such proposals so they would be aware of the research activity and could provide their expert opinion on the technical quality of the work. The NSF did not agree—as the NSA's Corry put it three weeks later—"to cooperate with us in considering the security implications of grant applications in this field."

In April 1978, the Senate Select Committee on Intelligence, which has oversight responsibility for the NSA, recommended—

That the NSF should decide what authorities and obligations it has to consider the national security implications of grant proposals;

That NSF and NSA should initiate efforts to reduce the ambiguity and uncertainty which surrounds the granting of research funds for public cryptography; and

That NSA and NSF should discuss the need for NSA to become part of NSF's peer review process for the review of grant proposals for research in cryptography or cryptanalysis.

The first of these recommendations reiterated what the NSA's Corry mistakenly claimed in May 1977 to have won by agreement with the NSF, and the third urged a peer review function for the NSA that had already been accorded. (In a footnote listing some regulations "of various types which are interpreted to have some effect on cryptology," the Senate committee unaccountably included provisions of the Atomic Energy Act (42 U.S.C. 2274–77) concerning communication, receipt, tampering with and disclosure of atomic enery Restricted Data.)

The second recommendation, on reducing ambiguity and uncertainty in the granting of research funds for public cryptography, perhaps spurred NSF Director Richard C. Atkinson to suggest to NSA Director Inman in September 1978 that "a small unclassified research support program at universities ($2–3 million, say) sponsored by NSA would help prevent future problems." Atkinson added, "If a mission agency supports a particular area of basic research, we can often reduce our effort in that area correspondingly," and volunteered NSF resources to help NSA set up such an operation.

This committee finds nothing in the history of NSA-NSF discussions and correspondence since April 1977 to evince an offer or willingness on NSF's part to abdicate its support of public cryptography. In the course of its inquiry, the committee has found no law, policy or regulation that would confer or underscore NSA's claims of dominion over research in public cryptography.

It also finds no shred of evidence to support a notion or claim that private ideas in cryptography are "born classified."

The committee has not tried to determine whether the National Security Agency tendency to advance exaggerated claims of authority in its dealings with the National Science Foundation stems from conscious policy or the actions of individual NSA employees.

6. Controls over the export of unclassified technical data pose a vague but constant threat to public cryptography. The controls are embodied in the Export Administration Regulations, which attempt to prevent the transfer of technical data that would adversely affect U.S. national security or foreign policy, and in the International Traffic in Arms Regulations (ITAR), which govern the export of unclassified technical data pertaining to arms, ammunition and implements of war on the U.S. Munitions List. The ITAR auxiliary military equipment category specifies speech scramblers, privacy devices and cryptographic devices (encoding and decoding).

Findings made by Congress in the Export Administration Act of 1979 include:

> It is important that the administration of export controls imposed for national security purposes give special emphasis to the need to control exports of technology (and goods which contribute significantly to the transfer of such technology) which could make a significant contribution to the military potential of any country or combination of countries which would be detrimental to the national security of the United States.

The Senate Committee on Banking, Housing, and Urban Affairs, which drafted the measure, said the definition of technology is

> intended to encompass everything contained within the term "technical data" and "technical services" as defined by regulation under the Export Administration Act of 1969, as amended.

That 16-month-old statement of congressional intent could be interpreted by the Department of Commerce as releasing it from an obligation to offer some regulatory relief. That would be unfortunate, especially since the Department in February 1980 demonstrated a willingness to invoke these export regulations to bar foreign scientists from a California conference on new computer technology. (Commerce officials relented under State Department entreaties, but then imposed conditions on the flow of technical data at the conference.) Also in February, the State Department issued a clarification of the ITAR controls on public cryptography that seems to clarify little while insisting that algorithms can be dangerous if they purport to have advanced cryptologic application. In any case, both sets of regulations place the burden on the would-be (or unknowing) scientific exporter to find out whether the technical data and the setting require an export license.

The researcher in cryptography stands at special risk of being found in violation of these export regulations, judged less by known enforcement activity than by the vagueness of the regulations and the National Security Agency's admonitions that extensive public work in cryptography and related fields can have a significant potential adverse impact—in a number of related ways—on national security.

In addition, there is a view gaining credence—in development of a militarily critical technologies list, for example—that domestic publication of research information is tantamount to its export and, therefore, that the only way to preclude export of such information is to restrict or prohibit its publication.

Another prospect—manifested in NSA's insistence that the National Science Foundation consider the national security implications of its cryptographic grant proposals—is that all such work might be deemed classified at the outset and therefore subject to the Government's will.

The committee is deeply concerned by these developments. It appears that they entail constitutional infirmities, yet they would enter an area—spanning invention secrecy, export controls and atomic energy Restricted Data—that is virtually devoid of constitutional testing.

Academic scientists work in a publish-or-perish environment. Publishing usually means reporting their work in a scientific or technical

publication, but it can also mean patenting. The patent route can be blocked by the Invention Secrecy Act, which allows the Commissioner of Patents and Trademarks to prohibit disclosure and withhold a patent in the name of national security. If publication of cryptographic research in scientific settings can be foreclosed as well, the Government will truly—by analogy from its power of eminent domain over land—have laid claim to all the cryptographic ideas within its jurisdiction.

7. The National Security Agency's dialogue with the academic community is a welcome development. The agency and the nongovernmental sector should become better acquainted as a result, and perhaps will find a basis for resolving problems of mutual concern. However, the committee has some reservations about the process and its potential outcome:

1. The public members of the Public Cryptography Study Group established by the American Council on Education—the forum in which the dialogue is taking place—have not been given all the facts they should have for informed debate. As of mid-September, they have not been given copies of the memorandum opinion from the Office of Legal Counsel in the Department of Justice to Dr. Frank Press, Science Adviser to the President, on the constitutionality under the First Amendment of the ITAR restrictions on public cryptography.

The memorandum opinion of May 1978 was not made public by either the Justice Department or Dr. Press (who treated it as predecisional legal advice not subject to release outside the Government). At the subcommittee hearing in March 1980, NSA Director Inman testified that both his agency's general counsel and Department of Defense general counsel disagreed with the opinion. At its February hearing, the subcommittee received testimony from and questioned Justice Department witnesses about the opinion.

The subcommittee declared the memorandum opinion to be a public document, and it is printed with the hearings. Meanwhile, study group members should be given copies of it. They are entitled to information that other parties to the dialogue have had for more than two years.

2. At the hearings, Admiral Inman characterized the dialogue as an attempt "to sort out what kind of regulation, not necessarily what kind of legislation, might meet both these needs, the needs of national security and the need on the opposite side to insure that the Government does not needlessly interfere with the conduct of basic research." He later added, "My sense to this point on where we ought to go is with a board that is composed of people from both sides but with significant expertise to be able to make judgments."

As the dialogue progresses, study group members should keep in mind that any prospective agreement that would legitimize Government interference (but not needless Government interference) with the conduct of basic research must guarantee First and Fifth Amendment rights. A system of self-regulation that settled for less would be no deal at all.

3. As a working procedure, the public members of the study group have accepted on faith the NSA's proposition that the heightened interest in public cryptography poses unnameable threats to national security, and are considering a system of prior restraint on publication.

B. Discussion

"It was then that I first learned that intelligence work, like virtue, is its own reward."—Ellis M. Zacharias, father of the Navy's present cryptologic organization.[1]

I. INTRODUCTION

Six secrecy orders in effect today cover cryptologic inventions made in the 1930's—"brilliant work" that "still warrants being protected."[2] Yet the ultimate in invention secrecy is to file no patent application at all and maintain the discovery as the deepest of trade secrets. So it is that the Signal Corps Patent Board decided in 1937 that two inventions by cryptologist William F. Friedman were so important that no patent applications should be filed. Indeed, Congress on five occasions has passed private laws awarding money to Government employees or their heirs for royalties foregone on secret cryptologic inventions—in 1935, 1937, 1956, 1958 and 1964—and four of these are worded to acknowledge inventions on which no patent applications were ever filed.

The United States Code makes it a crime—punishable by fine of up to $10,000 and/or imprisonment of up to 10 years—to knowingly communicate to an unauthorized person or publish classified information—

> (1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or
> (2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or
> (3) concerning the communication intelligence activities of the United States or any foreign government; or
> (4) obtained by the process of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes.[3]

The section says the terms "code," "cipher," and "cryptographic system" include in their meanings,

> in addition to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications;[4]

Secrecy about cryptology, David Kahn has written in *Foreign Affairs*, "has been the rule at least since the science became a permanent function of state through the establishment of letter-opening black chambers in the Renaissance, as a concomitant of the rise of

---

[1] Quoted in David Kahn, "The Codebreakers." The Macmillan Company, New York (1967), pp. 387–388. Zacharias was describing the small, highly secret organization functioning in Room 2646 of the "temporary" Navy Department building on Constitution Ave. in Washington, D.C., with which he trained for 7 months in 1926.
[2] Testimony of Admiral B. R. Inman, National Security Agency, in Hearings.
[3] 18 U.S.C. 798 (1976).
[4] Id.

modern diplomacy."[5] For example, he notes, Britain's House of Lords asserted in 1723 in a trial for treason that "it is not consistent with the public Safety, to ask the Decypherers any Questions, which tend to discover the Art or Mystery of Decyphering," and continues:

> Governments still adhere to this principle as much as they can. In 1933 and again in 1950, the United States enacted laws that impose fines and jail terms for anyone revealing official cryptologic secrets. The National Security Agency (NSA), responsible for U.S. cryptology, operates under the tightest possible security. The same is true of its foreign counterparts.[6]

The modern "Art or Mystery of Decyphering" is so closely held by the NSA that the term "public cryptography" may be misleading (at the hearings, author-editor Kahn proposed instead as more descriptive the term "nongovernmental cryptology," meaning work by private citizens to make and break codes[7]). To the extent there is a nongovernmental sector making cryptographic devices for export and generating associated technical data, it is restrained by other laws and regulations. The Department of State controls export to all destinations of unpublished data on the design, production or manufacture of arms, ammunition or implements of war on the U.S. Munitions List. These controls are applied through the International Traffic in Arms Regulations (ITAR).[8] ITAR Category XIII (Auxiliary Military Equipment) includes:

> (b) Speech scramblers, privacy devices, cryptographic devices (encoding and decoding), and specifically designed components therefor, ancillary equipment, and especially devised protective apparatus for such devices, components, and equipment.[9]

Category XVIII extends the ITAR to technical data relating to articles on the munitions list.

Under ITAR, an exporter of cryptographic devices and information must obtain a license from the State Department's Office of Munitions Control whether the actual exports are classified or not.[9a] These regu-

---

[5] Kahn. "Cryptology Goes Public." 58 "Foreign Affairs" 1, 142 (1979).

[6] Id., pp. 142–143. Kahn refers to 18 U.S.C. 798, added Oct. 31, 1951, and to the Act of June 10, 1933, 48 Stat. 122, now 18 U.S.C. 952 (1976), which reads, "Whoever, by virtue of his employment by the United States, obtains from another or has or has had custody of or access to, any official diplomatic code or any matter prepared in any such code, or which purports to have been prepared in any such code, and without authorization or competent authority, willfully publishes or furnishes to another any such code or matter, or any matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States, shall be fined not more than $10,000 or imprisoned not more than ten years, or both." This provision was aimed at the author of "The American Black Chamber," Herbert O. Yardley, and his manuscript of a second expose entitled "Japanese Diplomatic Secrets." United States marshals seized the manuscript on Feb. 20, 1933, at the offices of The Macmillan Company. See Kahn, op. cit. at 364.

[7] Testimony of David Kahn in Hearings.

[8] 22 CFR 121–128 (1980).

[9] 22 CFR 121.01 (1979).

[9a] The Data Encryption Standard (DES), which specifies an algorithm to be implemented in electronic hardware devices to be used for the cryptographic protection of computer data, is under the export control of the ITAR. "Cryptographic devices implementing this standard and technical data regarding them must comply with these Federal regulations," according to Federal Information Processing Standards Publication 46, U.S. Department of Commerce National Bureau of Standards, p. 2 (Jan. 15, 1977). It does not explain why a cryptographic standard intended for private sector and unclassified Government use is included on the U.S. Munitions List.

lations provide that licenses may be refused whenever issuance would be inadvisable in the interest of world peace, national security or foreign policy objectives. In fiscal 1978, exports of cryptographic devices—almost all speech privacy devices—were valued at $800,000. In fiscal 1979, they totaled $1.8 million.[10]

At the February hearing, the subcommittee placed in the hearing record and received testimony on a previously unpublished legal opinion—issued in May 1978 by the Office of Legal Counsel of the Department of Justice—on the Constitutionality under the First Amendment of ITAR restrictions on public cryptography. The opinion was addressed to Dr. Frank Press, Science Adviser to the President, and closed:

> In conclusion, it is our view that the existing provisions of the ITAR are unconstitutional insofar as they establish a prior restraint on disclosure of cryptographic ideas and information developed by scientists and mathematicians in the private sector. We believe, however, that a prepublication review requirement for cryptographic information might meet First Amendment standards if it provided necessary procedural safeguards and precisely drawn guidelines.[11]

At the March hearing, NSA Director Inman was asked if he viewed the OLC opinion as incorrect. The Admiral responded in part:

> Very much so. I argued very strongly at the time that I did not—I am not a lawyer—but after examining the merits of the case, I did not believe ITAR was so vague as to be unconstitutional, and I was therefore pleased to find a court decision that held that same view. That isn't to say it was a perfect document.[12]

Asked if the opinion prepared for Dr. Press was binding on NSA, Inman replied:

> It was not. There was some unhappiness in that forum when I brought forth the counterviews at the time. I was teasing my own general counsel on the way here. That I view as very proper on either side. You hire lawyers to give you opinions that will support the positions you have taken, and that was the case in both instances of the one you cite.[13]

Absent a clear judicial test, the major work of legal interpretation of export policy as applied to public cryptography in the OLC opinion, binding on NSA or not. In *United States* v. *Edler Industries, Inc.*, the defendants appealed their conviction for exporting without a license technical data relating to rocket and missile components. The Ninth Circuit said the defendants had "advanced a colorable claim" that the First Amendment protected the technical data they disseminated but ultimately rejected their argument, holding that the technical data exported related in a significant fashion to specific items on the

---

[10] Information obtained from the National Telecommunications and Information Administration of the Department of Commerce (April 1980).

[11] OLC Opinion at 17–18, printed in Hearings. (See text accompanying note 42 in the invention secrecy section of this report.)

[12] Hearings, (T'script p. 123) Inman is alluding to *United States* v. *Edler Industries, Inc.*, 579 F. 2d 516 (9th Cir. 1978), discussed below.

[13] Id.

U.S. Munitions List and that the statutory basis for export licensing regulations evinced "a congressional intent to delineate narrowly the scope of information" subject to export control.[14] After *Elder* the Office of Legal Counsel reaffirmed its ITAR opinion:

> Thus, while the Ninth Circuit's decision is helpful in resolving First Amendment issues with respect to blueprints and similar types of technical data used as a basis for producing military equipment, we do not believe that it either resolves the First Amendment issues presented by restrictions on the export of cryptographic ideas or eliminates the need to reexamine the ITAR.[15]

If publication is tantamount to export, then private citizens can export their cryptographic ideas simply by publishing them. A rival "Art or Mystery of Decyphering" might arise outside the black chamber, in full public view.

2. CRYPTOLOGY: PEERLESS INVENTION SECRECY

> This life's work, as extensive as it is intensive, confers upon Willian Frederick Friedman the mantle of the greatest cryptologist.[16]

William F. Friedman, later the Cryptologist of the Department of Defense and special assistant to the director of the National Security Agency before his retirement in 1955, made nine inventions from 1933 to 1944, two with the aid of Frank Rowlett. "Two were so secret," David Kahn recounted in 1967, "that no patent applications had even been filed. Four are held in secrecy in the Patent Office: three of these pertained to the Converter M–134–C, a rotor machine, and one to the Converter M–228." Three have issued as patents.[17]

The four Friedman applications remain secret to this day—along with two other inventions of the 1930's—under NSA-sponsored secrecy orders.[18] While the Invention Secrecy Act of 1951 and its forerunners have been useful in suppressing information about cryptologic inventions,[18a] they have not been needed for the most important inventions.

---

[14] The court explained: "We deem it unnecessary in this case to resolve the precise scope of that (First Amendment) protection. Assuming the full applicability of the First Amendment, invalidation of the federal controls on munitions is unwarranted because of the narrow statutory construction that we adopt." (See note 12.) In *United States* v. *Progressive, Inc.*, 467 F. Supp. 990 (W.D. Wis. 1979), the Government cited *Edler* in its appellee brief in support of its contention that "the courts have upheld prior restraints against the communication of technical data." (See discussion of *Progressive* in next section of this report.)

[15] Letter of Aug. 29, 1978, from Larry A. Hammond, Deputy Assistant Attorney General, to Col. Wayne Kay, Senior Policy Analyst, Office of Science and Technology Policy. In Hearings.

[16] Kahn, op. cit., at 393.

[17] Id. at 391.

[18] Testimony of Admiral B. R. Inman in Hearings. He testified that the NSA has 7 secrecy orders in force and that the seventh dates to 1967. (Two of the Friedman patent applications are Ser. No. 682,096, filed July 25, 1933, and Ser. No. 107,244, filed Oct. 23, 1936. The other two cover inventions made jointly with Frank B. Rowlett. See note 28 and accompanying text.)

[18a] To facilitate access to the approximately 4.4 million U.S. patents, they have been categorized into about 400 broad technological groupings, or classes, and 103,000 specific technological subclasses. A University of Santa Clara law student, Lee Ann Gilbert, matched the classes which the Patent and Trademark Office recognized as cryptography against the list of classes searched by the Patent Office Secret Group (Group 220) and was able to define the Secret Group's interest in cryptography to include: Code receivers, class 178, subclasses 89 and following; Code transmitters, class 178, subclasses 79 and following; Codes, class 178, subclass 113; and Teaching, class 35, subclasses 2 and following. She used two Department of Commerce publications: "Manual of Classification" III-13 (rev. perm. ed. 1979) and "Index to the U.S. Patent Office" 50 (1977). Gilberts copyright paper on invention secrecy, the source for this note, has been accepted by the Santa Clara Law Review for publication in the spring of 1981.

In those cases, no patent application is filed at all, leaving sheer secrecy as sole protector of the Government's proprietary interests.

Between 1935 and 1964, Congress passed these five private laws in settlement of rights or claims involving secret cryptologic inventions:

1. An act for the relief of Captain Russell Willson, United States Navy (Private Law 74–79, June 13, 1935), $15,000;
2. An act for the relief of Maude P. Gresham and Agnes M. Driscoll (Private Law 75–267, August 11, 1937), $8,960.55 to Gresham and $6,250 to Driscoll;
3. An act for the relief of William F. Friedman (Private Law 84–625, May 10, 1956), $100,000;
4. An act for the relief of Laurance F. Stafford (Private Law 85–494, July 22, 1958), $100,000; and
5. An act for the relief of Frank B. Rowlett (Private Law 88–358, October 13, 1964), $100,000.[19]

In recommending passage of the bill for the relief of Capt. Willson, the House Committee on Naval Affairs explained in part:

> The value to the Navy and to the Government of this invention cannot be measured in dollars and cents. Its value to the Government may be judged by the fact that it was used during the World War in all dispatches between the Navy Department and naval headquarters in London, including those concerning movements of transports, where its secrecy protected thousands of lives and millions of dollars worth of property.
>
> Being aware of comparative ease with which confidential and secret messages were intercepted and decoded by unauthorized persons, Captain Willson conceived and perfected this invention while on a tour of sea duty in 1916. For Captain Willson to have patented this invention would have destroyed its usefulness in that it would then have been open to public inspection; instead, he gave it to the Navy.[20]

In the case of Gresham, widow of Navy Commander William F. Gresham, and Driscoll, the Senate Committee on Naval Affairs explained:

> Commander Gresham invented a device that greatly increased the efficiency of an important part of the naval communication service. This device was of such a secret and confidential nature, and of such importance to the National defense, that the Navy Department confiscated it for the exclusive use of the Navy and prevented Commander Gresham from obtaining a patent thereon. If this invention had been patented its usefulness would have been destroyed, as it would then have been open to public inspection.[21]

It said of Mrs. Driscoll's role that

> The Navy Department has recently conducted a further investigation into the matter and is of the opinion that Com-

---

[19] In Hearings.
[20] H.R. Rep. No. 284, 74th Cong., 1st sess. (1935).
[21] S. Rep. No. 526, 75th Cong., 1st sess. (1937). The recommended award of $8,750 to Mrs. Gresham was reduced by the amount of a $59.45 overpayment in rental allowance to her late husband.

> mander Gresham was the sole inventor of the device, but that the fundamental cryptographic principles which the machine was designed to employ probably was (sic) conceived by Mrs. Driscoll and disclosed by her to Commander Gresham.[22]

The award to Friedman in 1956 culminated legislative efforts that began in 1951. The Department of the Army made two reports on Friedman relief proposals. Its first, on July 6, 1953, responding to a congressional request of October 18, 1951, for a legislative report, noted that some delay in preparation of the report was unavoidable "[b]ecause of the complicated factual situation and certain security aspects of the subject matter of the Friedman inventions. . . ." [23] In its first report, the Army suggested that $25,000 "should be adequate compensation for Mr. Friedman. . .," [24] but in its second report, of March 10, 1954, agreed that the proposed $100,000 payment "would not constitute more than adequate compensation for Mr. Friedman's loss." [25]

In its first report, signed by Secretary of the Army Robert T. Stevens, the Army said of Friedman's nine inventions:

> All the inventions relate to crytographic devices or machines. Procurement by the United States of devices constructed in accordance with the principles of Mr. Friedman's inventions has approximated $10 million, most of which occurred during the active phase of World War II, and has involved the use of substantially all his inventions.
>
> Under the circumstances of his employment it appears clear that the Government has at least a nonexclusive license in Mr. Friedman's inventions, Mr. Friedman retaining the right to otherwise exploit them. Because of security considerations, however, Mr. Friedman has been prevented from attempting to derive any gain from his inventions commercially or from foreign governments. In the case of the two applications which have matured into patents, Mr. Friedman was so restricted until the issuance of the patents or just prior thereto. Insofar as the other 5 applications and 2 inventions are concerned, Mr. Friedman is still prohibited from attempting to make any profit therefrom. Such prohibition will remain in effect as to each application until the Department determines that security considerations no longer proscribe their publication.[26]

---

[22] Id.
[23] S. Rep. No. 1815 (to accompany H.R. 2068), 84th Cong., 2d sess. 2 (1956).
[24] Id. at 4.
[25] Id. at 6.
[26] Id. at 3. A subcommittee of the Senate Judiciary Committee held a hearing on the Friedman relief bill, H.R. 2068, on Feb. 16, 1956. However, the hearing evidently was never printed, and the Senate Judiciary Committee file on the bill now kept at the National Archives does not contain a transcript of the hearing, although it does contain the transcript of a hearing on an earlier Friedman relief bill. In a staff interview on May 23, 1980, semiretired Washington, D.C., attorney Ernest F. Henry, who testified at the 1956 hearing, said the hearing "was open to the extent that it didn't divulge anything." Henry was representing the estate of Edward Hugh Hebern, who founded the country's first cipher machine company, in Oakland, Calif., and filed a $50 million claim against the military services in 1947 for using his basic ideas without compensation. The Government settled the claim in 1958 for $30,000. (Friedman died in 1959. See generally, Kahn, op. cit., and Ronald W. Clark, "The Man Who Broke Purple." Weidenfeld and Nicolson, London (1977).) His widow, Elizabeth Friedman, a cryptanalyst in her own right, died in November 1980. See appendix to Hearings.

Congress in 1958 voted a $100,000 payment to Safford, who founded the Navy's cryptologic establishment. Congress said the payment was

> in full satisfaction of all claims against the United States in connection with cryptographic systems and apparatus invented and developed by him while serving on active duty in the United States Navy which have been held in secrecy status by the United States Government.[27]

In 1964, Congress authorized a $100,000 payment to Rowlett, co-inventor of two of Friedman's nine inventions, in consideration of his transfer of property.

> consisting of all substantial rights to a patent within the meaning of section 1235 of the Internal Revenue Code of 1954, in full settlement for all rights in respect to his cryptologic inventions which are now or at any time have been placed in secrecy status by the War Department of the Department of Defense, including but not limited to all rights with respect to his inventions covered by Patent Applications, Serial Numbers 70,412 and 443,320, which were the subject of secrecy orders from the Department of Commerce, dated March 23, 1936, and May 16, 1942.[28]

The payments to Willson, Gresham and Driscoll, and Friedman expressly acknowledge cryptologic inventions on which patent applications were never filed, and the payment to Rowlett in full settlement for all rights to his inventions is "not limited to" those on which applications were filed and placed under secrecy orders. Indeed, the award to Safford is worded broadly enough to accommodate inventions never offered for patenting.

These inventors were recompensed through direct congressional action. No doubt there are other such inventors whose identities are known only inside the intelligence community.

In a June 1980 letter to members of the Public Cryptography Study Group,[29] an associate editor of "Cryptologia," a journal of mathematical cryptology, contended that the NSA "considers just about everything related to cryptology sensitive." He explained:

> In one case involving William Friedman, NSA classified a paper which had been freely circulated throughout the world for 30 years. . . . Prior to publication of David Kahn's "The Codebreakers" the director of NSA personally tried to prevent its appearance through appeals to the publisher. Kahn's book is a history, not a technical treatise, and was based on publicly available documents.[30]

---

[27] Private Law 85–494.

[28] Private Law 88–358. The numbered patent applications cover the two inventions he made jointly with Friedman.

[29] The Public Cryptography Study Group, established by the American Council on Education and funded by the National Science Foundation, is discussed below.

[30] Letter of June 10, 1980, from Cipher A. Deavours, Assoc. Prof. of Mathematics, Kean College of New Jersey, to study group cochairman Ira Michael Heyman, University of California-Berkeley. In Hearings, p. —. Deavours refers to Friedman's "The Index of Coincidence and Its Application in Cryptology." River Bank Laboratories, Geneva, Ill. (1922). For a discussion of these classification efforts and their effect on Friedman, see Clark, op. cit., at 196–199. (Under its preservation or "brittle book" program, the Library of Congress microfilmed Friedman's "The Index of Coincidence" on June 13, 1974. It is Microform No. 33777 in the microform reading room.)

He added:

> Due to the tremendously wide range of cryptographic systems in use at any given time, almost any selected concept could be declared critical knowledge. Further, one could justify the classification of such material merely on the grounds that somewhere a related cryptographic system is in use.[31]

That view has affected NSA's relations with the National Science Foundation.

3. A CODED MESSAGE TO THE NATIONAL SCIENCE FOUNDATION

In June 1975, a grantee of the National Science Foundation's Division of Computer Research (DCR) who also worked with the National Security Agency told a DCR official that

> NSA has sole statutory authority to fund research in cryptography; and, in fact, that other agencies are specifically enjoined from supporting that type of work.[32]

The official, Fred W. Weingarten, asked NSF general counsel to determine whether this was so:

> Since my program and others in the research directorate support research very closely related to, if not directly in cryptography it is important that we find out as soon as possible if we are acting counter to federal law. I'll hold up making any new grant in this field until you let me know.[33]

On June 19, the office of general counsel replied:

> We have been unable to locate any statute of the nature described in your memorandum of June 13, 1975. We also contacted NSA's legal office which knew of no such statute. NSA may have primary or exclusive authority pursuant to executive orders in connection with certain phases of cryptographic transmissions within the Government, but this has nothing to do with support of research.[34]

The matter did not rest there. On April 20, 1977, two NASA officials, Cecil C. Corry and David G. Boak, visited Weingarten to discuss NSF's support of cryptographic research. His account of the meeting relates:

> Early in the meeting they suggested that a presidential directive gave them "control" over all cryptographic work and that we were operating outside that directive. I stated that I had checked that matter nearly two years ago with our General Counsel and was told that there was no such directive involving research. They didn't mention that subject again except for a subsequent offhand remark that they would have to get a law passed.[35]

---

[31] Id.
[32] Memorandum of June 13, 1975, from the Program Director, Special Projects, DCR, to NSF General Counsel. In Hearings.
[33] Id.
[34] Memorandum of June 19, 1975, from Jesse E. Lasken, Assistant to the General Counsel, NSF, to Dr. Weingarten, DCR. In Hearings.
[35] NSF memorandom for files of May 2, 1977, from Fred W. Weingarten. In Hearings.

Weingarten's file memo about the NSA representatives' visit continues:

> They wanted to "coordinate," but didn't define the term very well. I agreed to send any proposals in cryptography I received to them for review, with the caveat that I could not accept any secret reviews—reviews of the form "Don't support this, but I can't tell you why."
>
> We explained two characteristics of NSF style which had a bearing on this issue.
>
> (1) We respond to the research needs of the field. This (sic), in the absence of a direct federal policy disallowing basic research support for cryptology, we would consider proposals in that field on their merit.
>
> (2) We operate in as open a manner as possible, and would not decline for other than fully documeneted scientific reasons.[36]

The NSF official then put down what he labeled "a strictly personal view of what is happening, confirmed in part, but not entirely by our conversation":

> First—NSA is in a bureaucratic bind. In the past the only communications with heavy security demands were military and diplomatic. Now, with the marriage of computer applications with telecommunications in Electronic Funds Transfer, Electronic Mail and other large distributed processing applications, the need for highly secure digital processing has hit the civilian sector. NSA is worried, of course, that public domain security research will compromise some of their work. However, even further, they seem to want to maintain their control and corner a bureaucratic expertise in this field. They point out that the government is asking NSA help in issues of computer security. However, unquotable sources at OMB tell me that they turned to NSA only for the short-term, pragmatic reason that the expertise was there, not as an expression of policy that NSA should have any central authority.
>
> It seems clear that turning such a huge domestic responsibility, potentially involving such activities as banking, the US mail, and cable television, to an organization such as NSA should be done only after the most serious debate at higher levels of government than represented by peanuts like me.
>
> Furthermore, no matter what one's views about the role of NSA in government; it is inescapable that NSF relations with them be formal. Informal agreements regarding support of areas of research or individual projects need to be avoided.[37]

Letters were then exchanged on the nature of NSA's review of NSF grant proposals. On May 11, 1977, Cecil C. Corry, NSA Assistant Deputy Director for Communications Security, wrote Dr. John R.

---

[36] Id.
[37] Id.

Pasta, Director of NSF's Division of Mathematical and Computer Sciences:

> As we discussed on 20 April 1977, NSA remains concerned about heightened interest and activity relating to cryptography and cryptanalysis in the private sector, and we are grateful for your willingness to cooperate with us in considering the security implications of grant applications in this field.
>
> As mentioned, we will be pleased to review proposals which directly relate to, or seem to impinge on, cryptographic matters, and will attempt to be more responsive than has perhaps been the case in the past. We recognize and accept the practical limitations you face when attempting to determine where some basic research, particularly in higher mathematics, may lead. In that regard, we can perhaps assist you in your review process for sponsored activity when the research appears to you to be in areas of NSA interest.[38]

Pasta forwarded the letter through channels on May 16, 1977, with a covering memorandum in which he explained:

> In the attached letter dated 11 May 1977, NSA asked us to keep them informed of proposed research in the crytology area. We have agreed to use NSA people as reviewers of such proposals so they will be aware of the activity and can provide their expert opinion on the technical quality of the work. I did not agree "to cooperate with [them] in considering security implications of grant applications", an activity for which I do not feel qualified. The substance of our discussion was sent to you in our earlier memorandum prepared by Fred Weingarten.
>
> In the last paragraph, they suggest that this monitoring be extended to other parts of the Foundation. This appears to be a matter to be pursued at some appropriately higher level.[39]

On November 28, 1977, Pasta replied to Corry, saying the letter "will clarify our understanding of the arrangements" discussed in their April meeting and in Corry's May letter:

> In the interests of interagency cooperation, it is our practice to keep other Federal agencies informed about program activities which are of interest to them. In line with this practice, we will attempt to send you for information purposes copies of proposals received by this Division which explicitly bear on cryptology. We consider this practice to be public releasable information.
>
> We would welcome any technical comment you might wish to offer concerning the content of any proposal. Please bear in mind that any such comment would be treated as a review, and it would become part of the documentation of the pro-

[38] In Hearings. Corry observed that NSF directorates "other than your own" evidently sponsor grants with cryptographic implications and wrote, ". . . perhaps you can arrange with them to have the Chief of the NSA Policy Staff, Mr. Norman Boardman, review their applications in the cryptographic field as well."

[39] Memorandum of May 16, 1977, from John R. Pasta. In Hearings.

> posal jacket. Unsigned verbatim copies of all reviews are sent to proposers upon their request. The Foundation considers proposals to be privileged documents until and unless we support the proposed research, and expects that they will be treated as such by reviewers and other recipients.[40]

Meanwhile, late in 1977, the Senate Select Committee on Intelligence undertook a classified study of allegations that the NSA was improperly involved in the development of a data encryption standard (DES) for certification by the National Bureau of Standards for use for all Government nonclassified data. A subsequent staff report of the study explained:

> The interest of the committee stems from its oversight responsibility for NSA and as a result of several allegations made about NSA harassment of scientists working in the field of public cryptology.[41]

In its study, the committee investigated allegations "that the NSA exerted pressure on officials in the National Science Foundation (NSF) to withhold grant funds for scholarly research in the field of crytology and computer security," and "that U.S. Government harassment brought about a chilling effect in universities doing research on cryptoanalysis and even resulted in one university withdrawing already published material from its library shelves." [42]

Based on its study,[43] the Senate Intelligence Committee concluded that:

> The NSA has not put pressure on the NSF to prevent funding of grants for cryptological research. However, the very uncertainty and ambiguity surrounding cryptology has prompted some NSA officials to express concern to NSF about certain grants with cryptological ramifications and to suggest that NSA be involved in reviewing these proposals. The NSF has agreed to the latter request, since it views NSA as the only location of competent cryptological expertise in the Government, but has not lessened its interest in, or willingness to fund, good proposals in this field.[44]

The intelligence committee also concluded that

> There has been no direct or indirect Government harassment of scientists working in the field of computer security. Nor has any university withdrawn library material as a result of NSA pressure. Nevertheless, the very newness of public cryptology and the vagueness and ambiguity of Federal regu-

---

[40] Letter of Nov. 28, 1977, from John R. Pasta, NSF, to Cecil C. Corry, NSA. In Hearings, p. —. As to Corry's request to "broaden the scope of this practice," Pasta wrote that he had mentioned the matter to Dr. Henry C. Bourne, Director of the Division of Engineering, and "you should feel free to contact him directly."

[41] Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard, Staff Report of the Senate Select Committee on Intelligence, 95th Cong., 2d sess. 1 (April 1978).

[42] Id. at 3.

[43] The classified study "is based on interviews with both public and private scientists and engineers, including representatives of the following government agencies, private companies and professional associations": NSA, National Bureau of Standards, NSF, Defense Department, International Business Machines, and "the Institute for Electrical Engineers and Electronics (IEEE)" (sic). "Over 200 pages of private and public papers and documents were also analyzed." Id. at 1.

[44] Id. at 3. This puts a different face on NSF's reasons for acceding to NSA's wishes. See notes 37, 39 and accompanying text.

lations pertaining to cryptology create an uncertainty which in itself is not conducive to creative scholarly work.[45]

In order to reduce "the potential capriciousness which is possible in ambiguous and uncertain situations," the committee recommended:

> That the appropriate committees of Congress should address the question of public cryptology by clarifying the role which the Federal Government should have in policies affecting public cryptology.
>
> That the NSF should decide what authorities and obligations it has to consider the national security implications of grant proposals.
>
> That NSF and NSA should initiate efforts to reduce the ambiguity and uncertainty which surrounds the granting of research funds for public cryptology.
>
> That NSA and NSF should discuss the need for NSA to become part of NSF's peer review process for the review of grant proposals for research in cryptography or cryptanalysis.[46]

In September 1978, NSF Director Richard C. Atkinson suggested to NSA Director Inman that "a small unclassified research support program at universities ($2–3 million, say) sponsored by NSA would help prevent future problems." Atkinson first referred to a "very helpful" September 1 briefing on NSA's operation, and noted that in the second part of that meeting a participant

> "outlined the nature of the dilemma we are in: what do we do if NSF-supported basic research begins to impinge on sensitive areas? We were unable to resolve this problem directly beyond the steps we have already taken to keep your agency currently informed. It did occur to me, however, that there may be a long-term initiative which might ameliorate the situation.
>
> As you may know, the support of basic research by mission agencies has decreased in recent years, and the Administration has been encouraging a reinforcement of that support. It seems to me that a small unclassified research support program at universities ($2–3 million, say) sponsored by NSA would help prevent future problems. If a mission agency supports a particular area of basic research, we can often reduce our effort in that area correspondingly. Thus, you could

---

[45] Id. at 4. In April 1978, when this 4-page unclassified summary was issued, the NSA imposed a secrecy order on Prof. George Davida's invention of a cipher device that protects computers from penetration by unauthorized individuals. See invention secrecy portion of this report on Davida's cipher device. Also, Clark (see note 26) contends that the NSA informed the Library of Congress in the late 1950's that a long readily available treatise on the German ciphers used in World War I was henceforth to be treated as classified "Confidential," and that it told Friedman his "The Index of Coincidence" was being upgraded to "Confidential" (op. cit. at 196–197). Also, in a footnote to this conclusion, the committee listed some regulations "of various types which are interpreted to have some effect on cryptology," including the ITAR and 18 U.S.C. 798, 952. It also listed Sec. 414 of the Mutual Security Act of 1954, 22 U.S.C. 1934, which was repealed on June 30, 1976, and replaced by Sec. 38 of the Arms Export Control Act, 22 U.S.C. 2778. Inexplicably, it also listed provisions of the Atomic Energy Act, 42 U.S.C. 2274–77, concerning communication, receipt, tampering with and disclosure of atomic energy Restricted Data.

[46] Id. at 4. As to the DES, the committee concluded, "NSA did not tamper with the design of the algorithm in any way." It recommended that the National Bureau of Standards "should continue to follow developments in computer and related technology in order to be aware of any developments which could lessen the security of the DES."

> support the work liable to be of interest to you and NSF support would undoubtedly be shifted. It may be that you would administer the program through ARPA or ONR.[47]

Atkinson offered NSF resources to help NSA set up such an operation, and wrote, "In any event, if you should decide to pursue this suggestion, I offer my cooperation, including a joint meeting with you, Frank Press, and Secretary [of Defese Harold] Brown." [48]

The director of NSA replied two weeks later, declaring:

> Your proposal that NSA assume responsibility for much of that work is most attractive. It should provide us the opportunity to manage the sponsorship of basic research activity required to serve the public interest effectively, and your offer to provide a senior program director to facilitate the transition is welcome.[49]

Admiral Inman added that "some homework . . . needs to be done here, and perhaps with other agencies involved in public sector cryptography." He said this effort should be completed by mid-October.[50]

In December 1978, NSF Director Atkinson wrote to the director of NSA again, saying "This follow-up note is to ask how the homework you mentioned is proceeding," and adding:

> My own interest in this matter stems from a conviction that each agency with scientific and technological concerns has a need and responsibility for maintaining contact with pertinent research at every research level including basic research. Your own area, being of the highest scientific and technical nature, naturally leans heavily on such research. I appreciate the fact that your agency has assembled a formidable array of talent for your intramural effort, but there may be benefits to be derived from interaction with unclassified peripheral basic research, as we discussed at our meeting.[51]

Atkinson renewed his offer to provide assistance to effect such a transition, "not only in the spirit of cooperation but also because it is perceived to be in the public interest with respect to our respective missions." [52]

The trail of correspondence supplied by NSF at the request of the Subcommittee on Government Information and Individual Rights in March 1980 ends at that point. The subcommittee hearing on the classification of private ideas in March 1980 featured a panel discussion of public cryptography with NSA Director Inman, Prof. George Davida and author-editor David Kahn, which is discussed below.

Now the relationship between the NSA and NSF has erupted in new controversy. The weekly journal *Science* disclosed in August 1980,

---

[47] Letter of Sept. 7, 1978, from NSF Director Atkinson to Vice Admiral Bobby R. Inman, Director, NSA. In Hearings. See table in the invention secrecy findings section of this report showing how support of basic research by mission agencies has decreased in recent years in relation to support by other agencies. Also, "ARPA" means the Defense Advanced Research Projects Agency, or DARFA, a separate Defense Department agency under the control of the Under Secretary of Defense for Research and Engineering. "DARPA has the responsibility to manage high-risk, high-payoff basic research and applied technology programs in projects as may be designated by the Secretary of Defense." United States Government Manual 1980–1981 at 245. "ONR" means Office of Naval Research.

[48] Id.

[49] Letter of Sept. 21, 1978, from Inman to Atkinson. In Hearings.

[50] Id.

[51] Letter of Dec. 27, 1978, from Atkinson to Inman. In Hearings.

[52] Id.

in an article in its news and comment section headed, "Cryptography: A New Clash Between Academic Freedom and National Security," that the NSF—at the NSA's prodding—last week

> told a computer scientist that it would withhold funds on certain parts of his cryptography research grant because they impinge on national security. This may be the beginning of a new sort of restraint on cryptography research.[53]

The article by Gina Bari Kolata reported that

> The latest development occurred on Thursday, 14 August, when Leonard Adleman of the Massachusetts Institute of Technology (MIT) and the University of Southern California got a telephone call from Bruce Barns of the NSF, who told him that parts of his grant proposal would not be funded. This is apparently the first time the NSF has refused funds to a researcher for reasons that have nothing to do with the merit of his proposal. When Adleman questioned Barnes further, he was told it was an "interagency matter."
>
> The interagency matter turns out to involve the relationship between the NSF and the NSA. It has implications which, to a number of academic scientists, appear particularly ominous.[54]

The article said that Acting NSF Director Donald Langenberg [55] refused to talk in any substance about his agency's relationship with the NSA, given his brief tenure, but that NSA Director *Inman* "talked freely with Science about his agency's contacts with the NSF," and continued:

> According to Inman, the reason the NSF chose not to fund parts of Adleman's grant proposal is that NSA wants to fund the research itself. The NSA, says Inman, first became interested in funding cryptography research when academic scientists started moving into the field. About 2½ years ago, Inman initiated conversations with the director of the NSF, then Richard Atkinson. "We got authority, good ideas, and help from Atkinson," he says. Since the heads of the two agencies began talking, the NSF has routinely sent all of its cryptography proposals to the NSA for review.
>
> Finally, the NSA was ready to initiate its own funding. Two NSF proposals looked ideal for the NSA to support. "I wrote to Langenberg suggesting that these would be good ones on which to start," Inman says. One of the proposals was from Adleman. The other was from Ronald Rivest of MIT, who is Adleman's colleague.[56]

---

[53] 209 *Science* 995 (Aug. 29, 1980). In Hearings. The New York Times reported the story Aug. 27, 1980, on page one ("Science Foundation's Aid Denied For Sensitive Research on Codes"), with acknowledgement to *Science*. Other recent "Science" articles on cryptography include "Prior Restraints on Cryptography Considered," 208 "Science" 1442 (June 27, 1980), and, in the research news section, "New Codes Coming into Use," 208 "Science" 694 (May 16, 1980), and "Testing for Primes Gets Easier," 209 "Science", 503, in Hearings.

[54] Id. at 995.

[55] Atkinson resigned as director of NSF on June 30. Langenberg was nominated June 3 to be Deputy Director.

[56] Id. at 995. Rivest was not much of a problem, according to Kolata, because he "had mistakenly submitted his proposal to renew his grant 1 year early. Barnes [of NSF] called Rivest and told him that he may hear from the NSA. So far, he has not."

According to Inman, the NSF was undecided on how to react to NSA's desire to fund Adleman. The article continues:

> The NSF, apparently, did not want to cut off his funds entirely while it wavered on the NSA's request, so it informed Adleman it would fund only part of his proposal—the part that did not interest the NSA.
>
> One day after hearing from the NSF, Adleman got a call from Inman, who explained that the NSA wanted to fund his proposal. Adleman was disturbed. "In the present climate, I would not accept funds from the NSA," he says. He worries about what terms the NSA might exact and points out that he applied to the NSF, not the NSA, and that he does not want any part of an implicit commitment to the NSA. He wonders what would happen if the NSA wanted to classify his work and he refused. Would his funds be cut off? If so, he believes he would have no due process. He is concerned about the NSF's agreement with the NSA. "It's a very frightening collusion between agencies," he says.[57]

Adelman is a theoretical computer scientist. His research, says Rivest,

> "has to do with a fundamental understanding of what it means for a computation to be hard or easy." Rivest is gravely concerned that the NSA wants to fund such research. "I'm shocked," he remarks. "What worries me is that the line [between what is and what is not cryptography] is being pushed in a way that affects our ability to do basic computer science research." [58]

In contrast to Inman, who seems quite clear about what his agency wants, writes Kolata, the NSF

> appears unable to make up its mind. "We're still trying to work out a policy [on cryptography research]," says Langenberg. But if the NSF continues to delay, its policy may end up being worked out for it, and academic scientists may find that, without any public discussions, there are prior restraints on their research.[59]

At the subcommittee hearing in March, in the three-way panel discussion, author-editor Kahn argued that "no limitation should be placed on the study of cryptography," [60] and Prof. Davida agreed. The NSA director said his initial reaction to the problems that arose in his first 8 or 9 months in office (including the Davida secrecy order) was

> that we clearly needed additional legislation and I set out to seek the views of those in the academic world and the business world where I thought there might be counterviews to try to understand their position.
>
> That dialogue has gone along pretty well. There are some efforts underway in collaboration at this point between the two

[57] Id. at 995–996.
[58] Id. at 996.
[59] Id. at 996.
[60] In Hearings.

opposing views to try to sort out what kind of regulation, not necessarily what kind of legislation, might meet both these needs, the needs of national security and the need on the opposite side to insure that the Government does not needlessly interfere with the conduct of basic research.[61]

The impression given by this history of NSA–NSF relations over the last 3½ years is not that of two agencies at loggerheads, but of the mission-oriented NSA having sent the NSF a message in bureaucratic code that the latter is still struggling to decipher. The record leaves little doubt about NSA's intentions.

4. THE NSA BREAKS ITS SILENCE

The first press interview by any director of the supersecret National Security Agency was given by Vice Admiral B. R. Inman to the journal *Science* in 1978.[62] Breaking with his agency's 25-year policy of public silence,[62a] Inman gave an exclusive interview following a series of four incidents "in which the NSA or its employees attempted to classify or limit unclassified research, development, and patent applications in communications privacy." [63]

Inman disclosed in the interview, published in October 1978, that he had asked for a "dialogue" with the academic community over the implications of new research in cryptography and communications security:

> "There's a real question now . . . given the burgeoning interest in this field, how to protect valid national security interests," Inman told Science. "One motive I have in this first public interview is to find a way into some thoughtful discussion of what can be done between the two extremes of 'that's classified' and 'that's academic freedom'."
>
> Inman explained that situations might arise where the NSA would want research performed on campuses or in the private sector to be classified. But the government has no power to do so beyond the patent and export laws, each of which cover (sic) specialized cases. *Inman* said there are "discussions . . . in limited parts of the Executive Branch" on whether NSA's legal authority could be extended without impinging on academic and other freedoms. He implied, but did not promise, that the Administration might propose legislation on the issue in coming months. "By the time we get through there will be a vast array of people in the Executive that will be drawn into this. There will be a debate between the Administration and the academic community," Inman said.[64]

---

[61] Testimony of Admiral Inman in Hearings.

[62] See Deborah Shapley, "Intelligence Agency Chief Seeks 'Dialogue' with Academics," 202 Science 407 (Oct. 27, 1978). In Hearings.

[62a] The NSA was created by a Top Secret memorandum from President Truman to the Secretaries of State and Defense on October 24, 1952. This directive remains classified even today. Prior to 1962, NSA's existence was not acknowledged in the U.S. Government Manual. It was not until 1975, 23 years after its creation, that any director of the NSA ever appeared before a congressional committee in public session.

[63] Id. at 407.

[64] Id. The progress of Executive Branch discussions is discussed below.

Inman commented from NSA's standpoint on two of the four incidents in which, he said, the agency had received a "bum rap." [65] These involved the NSA-requested secrecy orders issued on inventions by Prof. George Davida and by a group of four inventors led by Carl R. Nicolai. In the case of Davida's cipher devise, Inman said in the interview,

> the issuance of the secrecy order was a bureaucratic error, because, as it turned out, the material had already appeared in the open literature and so could not be classified. Under the procedures then in effect, he said, patent applications that are referred by the Commerce Department to the NSA were decided at the "middle management" level. "We did not have any internal system to challenge a decision to classify. This is a general problem of information across government. It's easy to classify and the question is how do you challenge the validity of it."
>
> After publicity in the press brought the Davida case to his attention, Inman began a new procedure by which any decision by middle management to request a secrecy order on a patent application would be automatically reviewed by a higher-level committee. This committee found that the secrecy order was not warranted.[66]

Science said the NSA director

> maintains that "there was a campaign that the imposition of the secrecy order interfered with the academic freedom of the investigators. I think that was a bum rap and I so told the Chancellor [Werner Baum of the University of Wisconsin-Milwaukee] by telephone. The decision to seek a patent conveys the intent not to share the information with others except for profit, which is the right of any inventor. . . . But if the individual had elected to publish in academic journals there would have been no question of a secrecy order." [67]

In the Nicolai case,[68] involving a device to scramble radio conversations, Inman told Science he personally had authorized the secrecy order:

---

[65] Id. Inman declined to discuss two other incidents. In one, an NSA employee, Joseph A. Meyer, threatened academic scientists with prosecution under the export laws if they discussed their research in cryptography. The other involved NSA's role in development of the DES (Id. at 410). The Senate Select Committee on Intelligence looked into the Meyer letter of July 1977 to E. K. Gannet, secretary of the Institute of Electrical and Electronics Engineers (IEEE) publications board. The April 1978 unclassified summary of its study declares that the committee "has determined that Mr. Meyer's letter to Mr. Gannet of the IEEE was inisiated solely by Mr. Meyer in his capacity as a member of the IEEE and was not prompted by any NSA official." In the DES matter, the committee found that NSA convinced International Business Machines that a reduced key size was sufficient, indirectly assisted in "development of the S-box structures" and certified that the final DES algorithm was free of any statistical or mathematical weaknesses, but that NSA "did not tamper with the design of the algorithm in any way." (See note 41 supra.)

[66] Id. at 407.

[67] Id. To seek a patent does not necessarily convey "the intent not to share the information with others except for a profit." For example, the Washington Post recently reported the claim of Goodyear Tire & Rubber Co. scientists to have found "a safe, cheap way to dispose of polychlorinated biphenyls (PCBs), one of the nations most pervasive toxic chemical wastes." Goodyear said it has applied for patents on the disposal process. "If granted, the patents will be turned over to the public at no cost, a spokesman said." (Aug. 22, 1980, p. E1).

[68] See chapter, "Squelching the Voice Scrambler," in the invention secrecy section of this report.

> The application "was reviewed under the new procedure and there was disagreement among the reviewing principals as to whether it merited classification or not. And, given the disagreement, I elected to ask for the secrecy order to be put on. Where there is uncertainty, I believe we should err on the side of national security.[69]

In general, Inman declined to answer the interviewers questions

> regarding what level of cryptographic and communications security devices the NSA would like to see allowed for use by Americans. He said any comment would bear on the "communications security" aspect of NSA operations which he would not discuss.
>
> But on the second issue, of whether first amendment rights can be reconciled with what NSA thinks necessary for national security, the NSA position does not seem so far afield from that sketched by spokesmen for the research community. Inman indicates that NSA would like authority like that the Atomic Energy Commission (AEC) (and its successor agencies) has under the Atomic Energy Act. Under the law, the AEC can classify the work of any American (and in one case they even classified the lecture of a Soviet citizen) that it thinks will jeopardize atomic energy secrets. Such clear authority does not exist, according to Inman, in the cryptologic area. In the past, Defense Department lawyers have told Science that such clear authority may not extend to any nonnuclear work with military applications.[70]

Three months later, in January 1979, Inman gave what he termed an "unprecedented" public address to the Armed Forces Communications and Electronics Association (AFCEA) as the "inaugural of a new policy of open dialogue with the public." [71] Traditionally, he noted NSA "has maintained a policy of absolute public reticence" concerning all aspects of its two-fold mission carrying out the signals intelligence activities of the Government and performing its communications security function. He explained:

> Until recently, the Agency enjoyed the luxury of relative obscurity. Generally unknown to the public and largely uncontroversial, it was able to perform its vital functions without reason for public scrutiny or public dialogue.[71a] NSA's

[69] Id. at 409.
[70] Id. at 410.
[71] Inman, "The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector." Speech delivered before AFCEA's January Vital Telecommunications Issues Symposium at the State Department, Washington, D.C. (1979). Printed in the AFCEA journal, 33 Signal No. 6 (March 1979). In Hearings.
[71a] Public scrutiny has revealed that in August 1945, immediately after World War II, the Army Signal Security Agency (later the Army Security Agency) implemented a plan that led ultimately to making most telegrams entering and leaving the United States available to that agency, whether coded or uncoded. ITT Communications and Western Union began their participation by Sept. 1, 1945, and RCA Communications by Oct. 9, 1945. For the next 30 years, until 1975, RCA and ITT—which together handled about 70 percent of all international nonverbal telecommunications in and out of this country—made their customers' communications available to the Army Security Agency or its successor, the NSA. Western Union's participation was shorter and more selective. See generally, S. Rep. No. 94–755. Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans, 94th Cong., 2d sess. (1976), Book III, and Interception of Nonverbal Communications by Federal Intelligence Agencies: Hearings Before a Subcommittee of the House Committee and Government Operations, 94th Cong., 1st and 2d sessions (1975–76).

particular field of technical mastery—cryptology—was of little public interest, except for a few hobbyists and historians.

This situation has now begun to change in important ways. One result of these changes is that the Agency's mission no longer can remain entirely in the shadows. Concern for the protection of communications, which for many years was viewed as being of interest solely in reference to government national security information, has now expanded throughout the government and to various important segments of the private sector. In the process there has developed a new and unprecedented nongovernmental interest in cryptology and in communications security. Expanded telecommunications protection activity, both governmental and private, has in turn led to an encounter between the activities of NSA and those of other governmental and private entities and individuals that in many ways is novel. . . .[72]

Inman stressed that he was

not saying that all nongovernmental crytologic activity is undesirable. To the contrary, the expansion of involvement in cryptology in the nongovernmental sector holds out the promise of significantly advancing the state of the cryptographic art in ways beneficial to both public and private interests. What I am saying, however, is that the very real concerns we at NSA have about the impact of nongovernmental cryptologic activity cannot and should not be ignored.[73]

Ultimately, he said, these concerns "are of vital interest to every citizen of the United States, since they bear vitally on our national defense and the successful conduct of our foreign policy."

He said "key developments and factors" include:

There is growing recognition of the potential vulnerability of our communications system within the United States to exploitation, both by foreign powers and domestic lawbreakers. . . .

There has been a growing public concern over the protection of data generated by or stored in computers. The public has become increasingly aware of the danger that automated data processing systems, if not adequately protected, can be exploited for fraudulent and illegal purposes. Moreover, the vast amounts of personal information stored in and handled by automated data systems, both private and governmental, has given rise to serious concerns about individual privacy. . . .

Impelled by the factors I have just described and acting under the authority of the 1965 Brooks Act, the National Bureau of Standards undertook to develop a data encryption standard (usually referred to as DES) to serve as the standard for protection, by encryption, of information in computers purchased or used by the Federal Government. The development of the DES is an area in which NSA has inter-

[72] Id. at 7.
[73] Id. at 7, 8.

acted with the non-national security segments of both governmental and private sectors. . . .

The existing statutory and regulatory framework for controlling the dissemination of potentially harmful cryptologic information has become embroiled in a certain degree of public controversy. Many of you no doubt are familiar with the concerns expressed by elements in the academic community that the nIternational Trafic in Arms Regulation (sic) (commonly called the ITAR) may serve to inhibit international exchanges of basic scientific information.

To cite another development, there has been a spate of recent scholarly activity in the cryptologic field. This has included publication of books and articles setting forth sophisticated attacks on commercially available cryptographic equipment, as well as the conduct of international seminars on cryptographic matters by noted U.S. experts.

Finally there are indications that companies are becoming interested in non-national security telecommunications protection as a promising new commercial market. While I have no basis for quantifying the size of such a market, I am aware that many forecast a substantial growth, both domestically and in terms of exports, in demand for cryptographic and other communications protection devices for non-national security applications.[74]

Saying he wanted to "set the record straight on some recent history," Inman declared the allegation that NSA had intervened in development of the DES was "totally false" and quoted approvingly from the unclassified staff report of the Senate Select Committee on Intelligence investigation of the affair.[75] He also termed "baseless" allegations that NSA "has attempted to suppress scholarly work in cryptology" through the use of the ITAR and the Invention Secrecy Act and by exerting pressure on the National Science Foundation, and noted approvingly that the Senate committee had found the Joseph A. Meyer letter-writing incident "was entirely a personal initiative." [76]

Inman acknowledged that the NSA

> has also recognized that ambiguities in the definitional provisions of the ITAR could be viewed as inhibiting international scholarly exchanges on matters relating to cryptology. Another ambiguity in the regulation could be viewed as imposing a requirement of prior governmental review on domestic scholarly publication. The Agency has taken the lead within the Executive Branch to attempt to clarify the ITAR so as to allay any fears that it may improperly apply to scholarly activity. As a result of NSA initiatives, I understand that the Office of Munitions Control is reviewing the matter

---

[74] Id. at 8–9.

[75] Id. at 9. Inman added, "The implausibility of the public allegations is further demonstrated by the fact that NSA has endorsed the use of DES for the encryption of national security-related information, including selected classified information."

[76] Id.

> and, if appropriate, will issue a clarifying statement that will meet the concerns expressed by the scholarly community.[77]

The NSA director said that in sponsoring secrecy orders under the Invention Secrecy Act,

> the Agency's sole consideration is the detrimental effect on the Agency's mission, and thus on the security of the United States, that would result from the proliferation abroad of sophisticated cryptologic technology.
>
> Equally baseless is the charge that NSA exerts some kind of undue influence on National Science Foundation research grant decisions. While NSA does play a peer review role with respect to such applications in the field of cryptology, that role has been limited to commenting on the technical merits of the proposal.[78]

These allegations and others that appear from time to time, Inman said, paint

> a false picture of NSA as exerting some kind of all-powerful secret influence all over the Government from behind closed doors. I can assure you from 18 months experience that this is far from reality. The truth is that the legal resources of the Federal Government to control potentially harmful nongovernmental cryptologic activity are sparse. Under the ITAR, the Government can prevent the export of harmful cryptographic equipment and some foreign dissemination of technical information having a direct relation to cryptographic equipment. There are, however, to my knowledge, no limitations whatsoever on publication of such nongovernmental information within the United States or on the export of such publications.[79]

The Invention Secrecy Act, he continued, provides a "very limited possibility of imposing secrecy on potentially harmful inventions"—limited because "the act applies only if an application for patent is made and, obviously, is effective only to the extent public disclosure has not already occurred before the secrecy order is issued."[80]

Admiral Inman said he believes the Government has too little power to control nongovernmental cryptologic activities:

> I believe that there are serious dangers to our broad national interests associated with uncontrolled dissemination of cryptologic information within the United States. It should be obvious that (NSA) would not continue to be in the signals intelligence business if it did not at least occasionally enjoy some cryptanalytic successes. Application of the genius of the American scholarly community to cryptographic and cryptanalystic problems, and wide-spread dissemination of

---

[77] Id. at 9, 12. The State Department issued a clarifying statement on "cryptography/technical data" in Munitions Control Newsletter No. 80 (February 1980).

[78] Id. at 12.

[79] Id.

[80] Id. Inman declared that in the application of the ITAR and the Invention Secrecy Act, "NSA plays a technical advisory role but is not the final decisionmaking authority." (Id. at 12). However, it should be noted that, under the Invention Secrecy Act, if the head of a defense agency requests issuance of a secrecy order, the Commissioner of Patents and Trademarks has no choice but to issue it.

resulting discoveries, carriers the clear risk that some of NSA's cryptanalytic successes will be duplicated, with a consequent inprovement of cryptography by foreign targets. No less significant is the risk that cryptographic principles embodied in communication security devices developed by NSA will be rendered ineffective by parallel nongovernmental cryptologic activity and publication. All of this poses clear risks to the national security. While I cannot go into further detail without exposing matters that must remain secret, I can tell you that I have not lightly accepted the position that unrestricted nongovernmental cryptologic activity poses a threat to the national security. . . .[81]

He said the concerns he had enunciated

> should not lead to the conclusion that nongovernmental cryptologic endeavor must somehow be halted. I think such a step would be a disservice to everyone. Similarly, any restriction on domestic dissemination of the fruits of such endeavors should be approached most cautiously and in a highly limited framework. With respect to exports of technology and equipment, I have much less hesitation. I believe that the present regulatory framework should be strengthened with respect to the export of cryptologic equipment and technical information having a direct relationship to such equipment. At the same time it should be clarified (and will be) so as to leave unfettered the free flow of basic research and scientific information among scholars in different countries.[82]

The NSA director suggested that if restrictions were to be placed on domestic dissemination of nongovernmental technical information relating to cryptology, they would have to meet "several criteria, for both policy and legal reasons," including:

> The restriction should apply only to a central core of critical cryptologic information that is likely to have a discernable adverse impact on the national security.
>
> Law and regulations should make these criteria as clear as possible without revealing information damaging to the national security.
>
> The burden of proof in imposing any restriction on dissemination should be borne by the Government.
>
> There should be judicial review of any such Government action, perhaps by a specially constituted court that could act under suitable security precautions, and the Government

---

[81] Id. at 13. D. Kahn writes in "For. Affairs" that there is one absolutely unbreakable cipher: "This is the one-time pad. It cannot be used in every situation because it requires as many random letters for its key as in all messages that will ever be sent, and this presents an insuperable distribution problem. It can serve in restricted situations, however, as in spy messages and on the Moscow-Washington hot line. There are also many ciphers that, properly used, are unbreakable in practice, since the cryptanalyst cannot assemble enough text to analyze their complexities. Because they do not have the disadvantage of the one-time pad, such systems serve in most military and diplomatic networks today." Computers, he adds, have not made it possible to solve all ciphers: "Modern cipher machines are in effect special-purpose computers themselves. Since doubling the encryption capacity appears to square the number of trials the cryptanalyst has to make, the codemaker can always stay ahead of the codebreakers." (Op. cit. at 145). See also, Roger Rapoport, "Unbreakable Code," 2 OMNI 12 (Sept. 1980).

[82] Id.

should bear the burden of obtaining judicial approval of its action.

There should be full, fair and prompt compensation for any company or person losing the economic benefit of information by virtue of governmentally-imposed restrictions on dissemination.[83]

In conclusion, Inman declared:

> Whether the risks to the national security that I have described today should lead to the imposition of any additional Government regulation is clearly a controversial question and one that remains to be fully examined by the Executive Branch, the Congress, and interested segments of the public. In my view, such examination should commence without delay and with the recognition that inaction is as much a choice as action in these circumstances. Any choice should be based on full consideration of all relevant information and views. In the coming months NSA will be undertaking discussions with the industrial and scholarly communities for purposes of better understanding the diverse points of view to be found in the private sector and, it is hoped, of stimulating consideration of alternative possible solutions. I solicit your participation in this process.[84]

The dialogue that Admiral Inman announced in October 1978 and expanded in January 1979 continued at the subcommittee hearings in March 1980 when he joined David Kahn, author of "The Codebreakers," and Prof. George Davida, recipient of a controversial NSA-sponsored secrecy order, in a panel discussion of public cryptography.

Inman testified that NSA's dialogue with members of the academic and business worlds "has gone along pretty well," and explained:

> There are some efforts underway in collaboration at this point between the two opposing views to try to sort out what kind of regulation, not necessarily what kind of legislation, might meet both these needs, the needs of national security and the need on the opposite side to insure that the Government does not needlessly interfere with the conduct of basic research.
>
> I am reasonably optimistic that this dialogue is going to produce information that will be of use to both the executive and legislative branches of Government. We deliberately, on both sides, have not sought publicity for that effort because we were eager to let the dialogue continue without the need to posture in public from either side.
>
> My encouragement comes from the fact that I have found particularly in the academic community great interest in the

---

[83] Id. With respect to courts acting "under suitable security precautions," it should be noted that the Department of Energy two years ago granted anticipatory clearances for atomic energy Restricted Data (Q clearances) to the Patent Office Board of Appeals and the U.S. Court of Customs and Patent Appeals. DOE did so to prepare for an appeal should a patent examiner reject its application to patent a laser isotope separation process. Such proceedings would be held in camera. (Staff interview with Anthony Campana, Technical Adviser, Office of the Asst. Gen. Counsel for Patents, DOE, Aug. 26, 1980.)

[84] Id. at 13. In connection with his testimony to the subcommittee at the March 1980 hearing, Inman submitted the text of a comparable address under the same title that he gave at an AFCEA meeting in Los Angeles on Feb. 12, 1979. In Hearings.

> prospect that any part of the Government might be willing to discuss with them in advance the form regulation would take instead of presenting them with a fait accompli.[85]

On the availability of cryptographic information, Inman said he appreciated copanelist Kahn's eagerness "to see this debate move forward in the public domain," but advised him not to expect major new revelations:

> Alas, I report to him that the files are not about to be thrown open and all that good detail on the success of the U.S. cryptologic community over the last 30 or 40 years. Where it can safely be done with regard to World War II adversaries, a great deal of information has been provided to the U.S. Archives. It will be a substantial period of time before other large volumes move into that category because there are continuing national security interests right to this day.[86]

Inman asserted that Congress already has made "some basic decisions about the importance of cryptography to the country and (has) provided some protection for it," starting with enactment of 18 U.S.C. 798.[87] Further, he said,

> in recent years they have taken what I believe to be a very wise step of creating the House Permanent Select Committee on Intelligence which has the requisite security and the requisite access to in fact examine and make judgments on the value to the nation, which my two distinguished colleagues Kahn and Davida do not have the opportunity to do, nor does this committee.
>
> I would suggest to you one of the things you might like to do would be to ask Chairman Boland and his committee to examine, and they certainly will not give you the detailed results, the detailed nature of the examination, but they would give you their own conclusions as to the question of impact on national security.
>
> They have already had some direct, firsthand experience on the question of whether the danger is overstated that publication in the U.S. of information will lead to the loss of vital information. They have seen the documented instances where it has occurred. Unhappily, the very nature of these hearings does not permit me to share those detalis with you. . . .[88]

The panelists disagreed on the question whether—given the explosion in telecommunications technology of the last 15 years—it is really possible to attempt to police the dissemination of ideas and technology, quite apart from whether policing of ideas is itself a good idea. Prof. Davida answered:

---

[85] In Hearings.

[86] Id. Archivists at the National Archives are not empowered to declassify cryptologic information that is more recent than World War I, and would not on their own recognizance declassify WW I information pertaining to U.S. efforts to break the codes of nonbelligerent nations. Section 3–403 of President Carter's EO 12065 reads, "Notwithstanding Sections 3–401 and 3–402 (which provide that classified information constituting permanently valuable records of the Government shall undergo systematic review for declassification), the Secretary of Defense may establish special procedures for systematic review and declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review and declassification of classified information concerning the identities of clandestine human agents." 14 Weekly Compilation of Presidential Documents 26 at 1201 (July 3, 1978).

[87] See text accompanying notes 3 and 4.

[88] In Hearings.

Mr. Chairman, I would like to address that because it is a very important question, assuming that we do want to restrict research.

Admiral Inman has raised the fundamental question about perhaps wanting to restrict applications as opposed to theory. I can simply say in computer science—I don't know how other disciplines might differ from it—very often there is little difference between theory and application. In fact, with the development of microprocessors it becomes trivial to take a procedure that someone develops theoretically and turn it into a machine that can encrypt.

I would say that that alone has given a great deal of capability to those who would like to encrypt their data. But more importantly, the microprocessor makes it possible to turn almost abstract ideas into machines overnight, and that can be done with the powerful high level languages, that have been developed.

Another thing in this area, it is difficult to draw the line between basic research and applications because there are many mathematical areas in computer science theory where there is a direct bearing on cryptography which would be difficult to restrict....

Mr. KAHN. Basically, I agree with Dr. Davida. It seems to me not only that it is impossible to attempt to police ideas but that it would be very deleterious and would harm the nation a great deal more than it would help it, as I set out in my paper.

Admiral INMAN. It would be indeed extraordinarily difficult to try to police ideas. The proposals that I have set forth in the dialogue would hold, as we do in our whole system of justice, that we look to obivously voluntary participation and support by those who would be regulated. I don't think it is workable unless they have in fact agreed to it.

But as a new student to this whole process, I have found thus far in my examination that none of the ideas which have come forth in the public sector are in fact new. The Government has either directly or with some of its collaborators examined usually some years ago each of those that have come forth thus far.

I find brilliant people who have tracked the developments in the computer world very skillfully for the Government benefit. One of the concerns has been whether the Government should fund general research in the academic world which has already been done by the Government.

The constraint immediately is how do you explain if it is classified that you have already done it once? My own sense is that much of the apprehension I find inside the National Security Agency comes from the fact that they know where their own thought processes have gone, and it isn't so much the threat they find now but where they believe some of these same bright minds may go in application 10 years from now, and the potential difficulty that brings to bear both on the

code and cipher systems, and on their conduct of the signals intelligence activities of the Government.

That activity I am not persuaded is necessarily going to be a Government province always. The motivation for me for the dialogue, and to get out to find out what is happening in that outside world, is the potential that this next decade will see some quantum jumps in the academic field, in the industrial field, which would catch up to what the Government has already done.[89]

Summed up, the NSA's public position is that (1) much historical information about this nation's cryptologic activities must remain under the archivist's lock and key, that (2) public cryptography so far has not broken new ground, that (3) academic and industrial scientists and engineers could take giant strides in the next decade that would erase the Government's classified lead in cryptographic applications; and that (4) a line must be drawn somewhere between Government needs and those of basic research.

Without fanfare, the NSA and the academic community have established a forum to determine where and how the line might be drawn.

5. THE PUBLIC CRYPTOGRAPHY STUDY GROUP

Concern over the April 1978 secrecy order imposed on Prof. George Davida at the request of the National Security Agency and NSA Director B. R. Inman's call for a dialogue with the academic community led the American Council on Education to convene a May 1979 meeting that recommended establishment of a Public Cryptography Study Group. The National Science Foundation agreed to fund it, and the group held its first meeting on March 31, 1980, in Washington, D.C.

All members were present, including Daniel C. Schwartz, NSA General Counsel, Prof. Davida, representing the Computer Society of the Institute of Electrical and Electronics Engineers, Ira Michael Heyman, Chancellor-Elect of the University of California at Berkeley, Jonathan Knight, Associate Secretary of the American Association of University Professors, and representatives of the IEEE, Association for Computing Machinery, American Mathematical Society and the Society for Industrial and Applied Mathematics.[90] The chairman was Werner A. Baum, Dean, College of Arts and Sciences, The Florida State University, who had been chancellor of the University of Wisconsin's Milwaukee campus when Davida received his secrecy order.

---

[89] In Hearing. Recent breakthroughs in the theory of cryptography enable the development of secret codes with an unprecedented characteristic: the method of encryption (the "key") may be made public without compromising the security of the communication. These public key cryptosystems (PKC) use two related but different keys: one for encryption, another for decryption. An analogy would be a lock on a mailbox with two combinations—one could be given to anyone wishing to put messages in, and the unlocking combination could be kept private to ensure that only the mailbox owner could open it and read his messages. By comparison, the data encryption standard (DES) is a traditional private key system. High-speed hardware implementations of the DES algorithm are readily available, while large-scale commercial availability of the PKC hardware is several years off. Also, known PKC algorithms are slower than DES. (From M. Merkhofer, S. Engle and C. Wood, "Decision Analysis Applied to a Technology Assessment of Public Key Cryptographic Systems," describing an SRI International project supported by a National Science Foundation grant. Menlo Park, Calif., 1980. The project is due for completion in January 1981.)

[90] Also present as authorized observers were Dr. Richard A. Leibler, Chief, Office of Research, Department of Defense; W. Todd Furniss, Senior Academic Adviser, ACE; representatives of NSF and the National Telecommunications and Information Administration, Department of Commerce; and a staff member of the House Subcommittee on Government Information and Individual Rights.

According to the minutes,[91] Chairman Baum concluded the initial discussion by raising the question of how the group should proceed, noting that the funding proposal to NSF

> had implied three steps: (1) a careful and precise articulation of the problems, (2) statements of positions on the issues, and (3) preparation of recommendations on how differences might be reconciled, to be submitted to the director of NSA and the president of ACE by the end of 1980.[92]

NSA's Schwartz agreed to prepare a statement of the issues to be addressed by the study group.

The group met next on May 29 with Heyman, U.C.-Berkely law professor and Chancellor-Elect, presiding as cochairman. Heyman reviewed the group's beginnings, recited NSA's concerns about potential threats to its mission, and summarized the NSA position:

> NSA looks on the present statutory tools as insufficient for minimizing these threats: (1) The Invention Secrecy Act involves only patentable devices and not information per se; (2) the Export Administration Act and ITAR involve only equipment and the information and technology directly related to it; they do not apply to knowledge and information in scholarly papers, articles, or conferences unrelated to specific hardware; (3) criminal statutes apply only to previously classified information. Finally, NSA seeks to explore some system analogous to that provided in the Atomic Energy Act, which proscribes publication or transmission of "restricted date" (sic) involving atomic weapons and related matters whether or not produced with government assistance. The system would be best if "voluntary."[93]

On the other side, Heyman noted that

> Some hold (1) that NSA has abused its present authority and (2) any limitations on non-public [i.e. private] cryptographic research, publication and development are unwise. The argument rests on the propositions (a) that cryptography is crucially important for civilian and non-intelligence operations and these applications would be weakened by any government controls; (b) non-public work is not actually harmful to the national security, or in any event such harm is counterbalanced by other considerations; (c) and the work in the private sector is very unlikely to lead to the breaking of NSA codes.[94]

The cochairman reminded the group that at its first meeting the NSA's Schwartz had suggested that to make any useful progress, the group should accept the proposition that public cryptography might

---

[91] The minutes are erroneously dated March 29. In Hearings.

[92] Id. The minutes record, "At this stage, no special effort will be made to publicize the Study Group's activities or to avoid publicity." (Notes taken by the subcommittee staff member who attended as an authorized observer record—but the minutes do not—that DOD's Dr. Leibler said NSA would take over the funding of cryptographic research grants from NSF, assuming there are no legal impediments to such transfer and the study group produces worthwhile recommendations on how to effect it.)

[93] In Hearings. Additional authorized observers at the May meeting included Prof. Cipher A. Deavours, Dept. of Mathematics, Kean College of New Jersey, and Gina Kolata, staff writer, Science magazine.

[94] Id. at 1–2.

under some circumstances imperils national security, that because of security restrictions this proposition has to be taken on faith, and that it is possible to accept this proposition provisionally. From that starting point, Heyman said, the group might proceed "to define as specifically as possible what a set of processes would apply to (and what they would not apply to), the processes themselves, and the tribunals responsible for them." [95] He asked for examples of the devices, technology and information at issue:

> For a time the discussion ranged widely as the group sought to define and describe the relationships between devices and algorithms, cryptologic devices and other devices covered by the various acts, and the criteria (protection of privacy, health, the environment, and property, in addition to preserving national security) that . . . might trigger governmental control measures. The discussion seemed to underline the absence of agreement even among federal agencies about what is or should be covered by the statutes in the field of cryptology. Nevertheless, the discussion clearly indicated that the core of the question before us was whether some form of prior restraint on publication of research results and other information relating to cryptology is necessary, feasible, and desirable.[96]

Heyman then called for a vote on the question, "That the group proceed on the basis that we will consider a system of prior restraint concerning publication of articles and other materials related to cryptography, reserving until the details of such a system are elaborated, any final decisions on whether such a system would be desirable." It passed, 7–1.[97]

Whether the study group determines that a system of prior restraint is legal, feasible and desirable remains to be seen, not to mention the degree of voluntary acceptance such a system would need in the academic community to be successful from the NSA standpoint.[98] The study group met again Oct. 6 in Menlo Park, Calif., and anticipates meeting early in 1981 to consider a final report.[99] At any rate, the

[95] Id. at 2.
[96] Id.
[97] Id.
[98] After attending the May meeting as an authorized observer, Prof. Cipher Deavours wrote, "The study group contains some very distinguished individuals, out, as, I think, most of them would admit, few af them have any knowledge of cryptology. This is, in essence, like gathering a group of biologists to assess research in physics. Some of the committee's members are now, or have been, consultants for NSA—this hardly makes them impartial as regards this matter. If we consider the seriousness of a concept like prior restraint from publication in a free society, it is seen to be imperative that persons conversant with cryptology and who, in addition, are non-governmental be included when the committee does its work." Letter of June 10, 1980, from Deavours to study group cochairman Heyman. In Hearings.
[99] In October the group took up the report of its subcommittee on procedures, chaired by Heyman, which proposed an approach that "is largely, but not completely, voluntary. Protected cryptographic information would be defined as narrowly as possible. Authors and publishers (including professional organizations) would be asked on a voluntary basis to submit prospective articles containing such information to NSA for review. If NSA staff found no difficulty (or if any questions that arose were resolved satisfactorily) publication would follow. If there were disagreements, an Advisory Committee would review the article and make a recommendation to the Director of NSA whether or not the government should seek to restrain publication. The Advisory Committee would consist of five cleared members—two appointed by the Director of NSA and three (from outside government) appointed by the Science Adviser to the President. There would be strict time limits on NSA staff and on the institution of any action to restrain publication." (Report of Subcommittee on Procedures, Sept. 29, 1980. The proposal was outlined in a four-page attachment. In Hearings. The two pages of minutes of the Oct. 6 meeting record that "(a)t the end of the morning session it was agreed that Heyman, assisted by the Subcommittee on Procedures, will prepare a revised and expanded recommendation for the voluntary approach."

dialogue Admiral Inman called for two years ago appears to be running its course.

6. EXPORT CONTROL POLICY

A. A Brief History of Export Controls

In the 1950's, American scientists mailing unclassified scientific information to scientific friends abroad were required to stamp their correspondence "Export license not required," to indicate they were aware of export regulations and had not violated provisions of the general export license. Under section 3(a) of the Export Control Act of 1949,[100] the Department of Commerce had claimed authority to control the export of technical data as well as commodities, and interpreted "technical data" to include basic scientific information.

The two stamps which scientists and technicians were supposed to use were:

GTDS
(General Technical Data Scientific)
(Export License Not Required)

GTDP
(General Technical Data Published)
(Export License Not Required)

In 1956, in its Twenty-Fifth Intermediate Report, the House Committee on Government Operations recommended:

> Section 3(a) of the Export Control Act of 1949 should be amended to make it clear that the phrase "technical data" does not include scientific information of an unclassified nature. This would abolish the regulation requiring American scientists to stamp their unclassified correspondence with scientists overseas.[101]

After the committee's recommendations were forwarded to the Secretary of Commerce, the department finally revised its regulations to permit foreign mailing of nonclassified scientific and technical data if the material was sent by first-class mail by a person without "commercial" connections. Violation of the vague requirements by a scientist seeking to exchange nonclassified research with his foreign counterpart could result in a criminal penalty of a $10,000 fine or a year in jail. In its Thirty-Fifth Report, the committee noted that its Subcommittee on Government Information was continuing to receive complaints from scientists about the restrictive regulations, and reported:

> After a letter from the subcommittee, explaining once again the importance of the free flow of nonclassified research material and pointing out that President Eisenhower had emphasized the need for international exchange of scientific information, the Commerce Department on March 7, 1958, again revised its regulations. Although the license categories covering the export of scientific and technical information still exist, scientists can now use any class of mail for their letters.[102]

---

[100] Act of Feb. 28, 1949, 63 Stat. 7.

[101] H. Rept. No. 2947. Availability of Information from Federal Departments and Agencies. 84th Cong., 2d sess. 92 (July 27, 1956).

[102] H. Rept. No. 2578. Availability of Information from Federal Departments and Agencies (Progress of Study, February 1957–July 1958), 85th Cong., 2d sess. 18 (Aug. 13, 1958). The portion of that report headed "Export of Unclassified Scientific and Technical Information," pp. 17–28, is reprinted in Hearings.

The 1949 act was the first comprehensive system of export controls ever adopted by the Congress in peacetime. "Even that Act was initially conceived as a temporary measure, and might well have been allowed to lapse in 1951 but for the Korean War. The Export Control Act was renewed in 1951, and again in 1953, 1956, 1958, 1960, 1962, and 1965." [103]

Controls established in 1949 on all exports to Communist countries were gradually relaxed in the late 1950's and throughout the 1960's. The initiative for change came from the Congress, spearheaded by the Export Administration Act of 1969,[104] which replaced the Export Control Act entirely. The new act

> maintained export controls, but called for a removal of controls on goods and technology freely available to Communist countries from non-U.S. sources and on items that are only marginally of military value. The 1969 legislation represented a new mandate for export controls. Whereas the thrust of the Export Control Act of 1949 had been to limit East-West trade, the 1969 Act was designed to foster such trade.[105]

Export controls have been an important issue in each Congress of the 1970's. The Export Administration Act of 1969 was significantly amended in 1972, 1974 and 1977, and superseded by the Export Administration Act of 1979.[106] The 1979 law maintained the basic emphasis on export expansion that was introduced by the 1969 act.

B. Exports of Technical Data by Publication

Section 120 of the Export Administration Amendments of 1977 required the Secretary of Commerce to

> conduct a study of the transfer of technical data and other information to any country to which exports are restricted for national security purposes and the problem of the export, by publications or any other means of public dissemination, of technical data or other information from the United States, the export of which might prove detrimental to the national security or foreign policy of the United States. Not later than 12 months after the enactment of this section, the Secretary shall report to the Congress his assessment of the impact of the export of such technical data or other information by such means on the national security and foreign policy of the United States and his recommendations for monitoring such exports without impairing freedom of speech, freedom of press (sic), or the freedom of scientific exchange.[107]

---

[103] Harold Berman and John Garson, "United States Export Controls—Past, Present, and Future." 67 Columbia Law Review 5 at 792 (May 1967).

[104] Act of Dec. 30, 1969, Public Law 91–184, 83 Stat. 841, 50 U.S.C. app. 2401 (1976).

[105] In "Export Controls: Background and Policy Analysis." Issue Brief 75003, Congressional Research Service, Library of Congress (March 24, 1980). The new legislative mandate did not eliminate controls on technical data. For example, an unclassified 1970 technical report of the Naval Undersea Center, "Some Hydrodynamic Measurements On Sharks," NUC TP 189) bears the cover legend, "This document is subject to special export controls and each transmittal to foreign governments or foreign nationals may be made only with the prior approval of the Naval Undersea Research and Development Center, San Diego, Calif. 92132."

[106] Act of Sept. 29, 1979, Public Law 96–72, 93 Stat. 503, cited as 50 U.S.C.

[107] Act of June 22, 1977, Public Law 95–52, 91 Stat. 235. Sec. 120 gave the Secretary the option of including this special report in a regular semiannual report to the President and the Congress, and the Secretary took it.

The report, "Exports of Technical Data by Publication or Other Means of Public Dissemination," was submitted to Congress early in 1980.[108] The executive summary of the report declares:

> The Department's assessment is that while technical data of conceivable adverse significance to U.S. National security and foreign poicy are on occasion publicly available, the impact of their availability on the U.S. national security or foreign policy is likely to be minor. This conclusion is based on the premise that availability does not generally result in an effective transfer of technical data. The availability of technical data with no interaction between those providing and those acquiring the data is usually a relatively ineffective means of transferring technology.
>
> Moreover, most publicly available technical data do not describe state-of-the-art technology. The availability of such technoolgy is carefully restricted by the business community for proprietary reasons and by the U.S. Government for national security and foreign policy purposes.
>
> Additionally, the public availability of technical data, in and of itself, does not overcome built-in obstacles to the absorption of that technology within another country and its diffusion throughout that nation.[109]

Monitoring publications and other means of public dissemination of technical data in the United States, the summary continues, would

> require the creation of a new governmental capability, including a staff of technical experts, to analyze, catalog, and index the information reviewed. In assessing the feasibility of implementing a monitoring system, a number of factors are weighed in this report: (1) what would be the purpose of monitoring; (2) the system's likely effectiveness; (3) the impact on the development and exchange of technical data and scientific information within the United States; (4) the cost; and (5) the legal and constitutional implications, including the impact on freedom of speech and freedom of the press.[110]

The report concludes that monitoring the public availability of technical data would be largely ineffective and unlikely to provide any real benefits. Further, a monitoring system would be extremely costly even on a modified scale, could adversely affect the development and exchange of scientific and technical information, and would raise legal and constitutional questions.[111]

In the Export Administration Regulations, the term "technical data" is defined as:

> . . . information of any kind that can be used, or adapted for use, in the design, production, manufacture, utilization, or reconstruction of articles or materials. The data may take a

[108] The report appears as Appendix D to 116th Report on U.S. Export Controls to the President and the Congress. U.S. Department of Commerce, Government Printing Office (1980).
[109] Id. at 128.
[110] Id. at 128–129.
[111] Id. at 129.

> tangible form, such as a model, prototype, blueprint, or an operating manual; or they may take an intangible form such as technical service.[112]

The report explains that transfer of technical data is of national security concern

> when it is likely to enhance the military potential of another nation in a manner that would be prejudicial to U.S. national security or the security of our allies. This can occur either when the technical data provide the technology to develop or upgrade the military equipment of a potential adversary or when they provide insights into U.S. military capabilities so that countermeasures can be developed.
>
> Foreign policy concerns arise when the transfer of technical data would enhance another nation's capabilities in a manner inconsistent with our foreign policies (for example, by enhancing the ability of a government to violate fundamental human rights or by threatening a neighboring country friendly to the United States) or when simply permitting any kind of transfer might be viewed as endorsement of a government whose overall policies are contrary to U.S. interests.[113]

To prevent the transfer of technical data that would adversely affect U.S. "national security or foreign policy," the Export Administration Regulations require exporters to obtain a validated export license—one requiring specific Government review and approval—prior to the export of most unpublished technical data to a potential adversary or other restricted destination. Data that are generally available to the public in any form may be transferred freely to all destinations under a general license and do not require specific Government review.[114]

---

[112] 15 CFR 379. 1(a)(1979). Sec. 379.3 establishes a General License GTDA authorizing the export to all destinations of the following technical data:

(a) *Data generally available.* Data that have been made generally available to the public in any form, including: (1) Data released orally or visually at open conferences, lectures, trade shows, or other media open to the public; and (2) publications that may be purchased without restrictions at a nominal cost or obtained without cost or are readily available at libraries open to the public. The term "nominal cost" as used in paragraph (a)(2) of this section is intended to reflect realistically only the cost of preparing and distributing the publication and not the intrinsic value of the technical data. If the cost is such as to prevent the technical data from being generally available to the public, General License GTDA would not be applicable.

(b) *Scientific or educational data.* (1) Dissemination of information not directly and significantly related to design, production, or utilization in industrial processes, including such dissemination by correspondence, attendance at, or participaton in, meetings; or (2) Instruction in academic institutions and academic laboratories, excluding information that involves research under contract related directly and significantly to design, production, or utilization in industrial processes.

(c) *Patent Applications.* Data contained in a patent application prepared wholly from foreign-origin technical data where such application is being sent to the foreign inventor to be executed and returned to the United States for subsequent filing in the U.S. Patent and Trademark Office. (No validated export license from the Office of Export Administration is required for data contained in a patent application, or an amendment, modification, supplement or division thereof for filing in a foreign country in accordance with the regulations of the Patent and Trademark Office in 37 CFR Part 5. See sec. 370.10(j).)*

* 15 CFR 370.10 reads, "Exports which are not controlled by the Office of Export Administration" Paragraph (j), below, was added and paragraph (c), above, was amended by the International Trade Administration on July 30, 1980 (45 FR 50556–57) to clarify the jurisdiction of the Patent and Trademark Office in licensing exports of patents and amendments or supplement thereto:

(j) *Patent Applications.* Regulations issued by the Patent and Trademark Office in 37 CFR Part 5 govern the export of a foreign country of unclassified technical data in the form of a patent application or an amendment, modification, or supplement thereto or division thereof. These regulations are issued under the authority of 35 U.S.C. 6, 181–188.

[113] Appendix D at 130.

[114] Id. at 130. These procedures apply to data relating to dual-use items, i.e. items that can have both civilian and military uses. Export of unpublished data about arms, ammunition or implements of war on the U.S. Munitions List is controlled to all destinations by the State Department under the ITAR (22 CFR 121–128).

In this context, the report on transfer of technical data treats "monitoring" as consisting of post-publication review without any attempt to control or restrict public availability. It then assumes that public availability here "is tantamount to their export to all destinations, including countries to which exports are controlled for national security or foreign policy purposes," and gives such examples as:

> A visiting scientist can attend a trade show open to the public and collect various business brochures and carry them back to his country.
>
> Members of foreign embassies can subscribe to the technical journals published regularly by numerous professional societies. These can easily be made available to scientific institutions in their own countries.
>
> By visiting an outlet of the U.S. Government Printing Office, a foreign business person can purchase the latest technical and scientific publications of the National Technical Information Service (NTIS). These publications often deal with high-technology subjects.[115]

Using NTIS estimates, the report reckons that 1.5 million scientific and technical reports were published in the U.S. in 1978, that 100,000 reports are presented annually at scientific meetings, and that another 160,000 documents involving patents and current research projects should be considered as sources of technical data.[116]

The report reasons that monitoring "would undoubtedly have an inhibiting effect on the development and exchange of scientific or technical information":

> Scientists concerned about censorship because their studies might involve material that is sensitive from a national security or foreign policy standpoint might avoid doing research in these areas. They might avoid areas where the U.S. Government would be likely to monitor their activities or where their research might subsequently become the object of government attention. Because their research might inadvertently reveal information of significant national security or foreign policy concern, researchers might be hesitant to develop certain types of scientific or technical projects without first consulting with the U.S. Government. This hesitancy might even create a reluctance to make scientific or technical information publicly available without prior consultation with U.S. Government officials.
>
> U.S. Government monitors looking over the shoulders of members of the technical and scientific community could instill a cautionary and restrained attitude in individuals whose strengths are their innovative, imaginative, and creative talents. The adverse consequences for the development of scientific and technical information and exchange could be far-reaching.
>
> The possibility of seriously inhibiting scientific and technical research and exchange of information is not confined

[115] Id. at 131.
[116] Id. at 133.

> to monitoring technical data related to national security or foreign policy. Since a wide range of data would have to be reviewed to determine whether national security or foreign policy concerns are raised, broad-gauged and ultimately unnecessary monitoring could ensue.[117]

Pre-publication governmental review and control of sensitive technical data "would obviously be a more effective way of preventing exports than post-publication review and control," the report observes, adding:

> Such a system of censorship, however, would raise serious First Amendment questions, would have a significant adverse impact on technical and scientific advance, and would entail greatly expanded administrative costs.[118]

The report concludes that while in certain instances technical data of consequence for national security or foreign policy may be available through publications and other means of dissemination, their overall impact on national security or foreign policy

> is probably minor. This conclusion is based on the assessment that public availability of technical data, in and of itself, is unlikely to result in the effective transfer of technology. Further, the Department believes that the technical data most critical to our national security and foreign policy are state-of-the-art technologies involving detailed production and design know-how, and that such data are not typically publicly available, since they are safeguarded either by commercial or governmental proprietary arrangements or by government classification restrictions.
>
> Because monitoring the export of sensitive publicly available technical data would (1) be largely ineffective and unlikely to provide any real benefits, (2) be extremely costly, even on a modified scale, and (3) have serious adverse consequences for the development and exchange of scientific and technical information, the Department of Commerce recommends against establishing a monitoring system.[119]

Less than a month after submitting its report to the Congress, the Commerce Department applied the Export Administration Act to bar Soviet and East European scientists from a California conference on bubble memories, an important new computer technology, sponsored by the American Vacuum Society. According to the journal *Science*,[120] the disinvitation incident seems to have begun when the Central In-

---

[117] Id. at 136–137.

[118] Id. at 139. The committee concurs in this analysis, but faults the report's subsequent assertion that technical data "do not fall into the traditional categories" of speech accorded First Amendment protections, as if they had been examined and found constitutionally wanting. Technical data have not been judicially tested. For example, the memorandum opinion on the constitutionality of ITAR restrictions on public cryptography by the Office of Legal Counsel, Department of Justice, in May 1978 (see note 11 and accompanying text) observes, ". . . it does not appear that the broad controls over exports of technical data and related information under the Export Administration Act of 1969, 50 U.S.C. 2401 et seq. (1970), and accompanying regulations have been judicially tested on First Amendment grounds." (In Hearings, p. —). See also notes 14, 15 and accompanying text on the relevance of *Edler*.

[119] Id. at 142. (The committee notes a printing omission on p. 141 of the report at line 3, in a paragraph discussing the *Progressive* case. The intended line was dropped and line 14 below has been mistakenly repeated at line 3.)

[120] Nicholas Wade, "Science Meetings Catch the U.S.-Soviet Chill," 207 Science 1056 (Mar. 7, 1980). In Hearings.

telligence Agency approached the society's New York office and asked for a copy of the program of the February 20–22 meeting in Santa Barbara:

> A few days later a bureaucratic nightmare began for the American Vacuum Society's president, John L. Vossen of the RCA Laboratories in Princeton. The conference organizers called from Santa Barbara to say they had been instructed by the Department of Commerce to disinvite the Soviet, East European, and Chinese delegates, and furthermore that all foreign nationals attending must sign a pledge not to disclose the information they heard to the nationals of some 15 other countries.
>
> Then the State Department got into the act. It didn't want the Chinese disinvited. The officials of the Office of Export Administration refused to be budged from their regulations, which said no Chinese. The Commerce position prevailed. Vossen hoped to disinvite no one. It was indicated to him that an offense against the Export Administration Act is punishable by a $10,000 fine and 1 year in jail. He decided to wire the disinvitations as directed.
>
> The Russians and East Europeans got the cables, which were sent on 15 February, but the Chinese were already in transit. They showed up in Santa Barbara on 18 February eager to discuss bubble memories . . .
>
> Their mere arrival in the United States, however, strengthened the State Department's hand in its tussle with Commerce. By 2 p.m. on 20 February, the first day of the meeting, a cable from the Commerce Department informed the organizers that the Chinese could be admitted, subject to a number of conditions. The technical data discussed at the conference were to be either already available in the public literature or, if unpublised, were to pertain only to general trends, not to manufacturing details. Also, all foreign scientists attending the meeting would have to sign a pledge not to divulge any unpublished information gleaned at the conference to any Eastern bloc national.[121]

The article said the Commerce Department believes its intervention has a sure legal basis:

> "If the information is technical data which is not in the public domain, a license might be required. As I read the law, I would need an export license just to engage in chit-chat about such data," comments an official of the Office of Export Administration.[122]

---

[121] Id. at 1056.

[122] Id. at 1056. From April through September 1979, Commerce approved 84 applications for the export of unpublished and unclassified technical data to the U.S.S.R., Eastern Europe and the People's Republic of China. It also approved 5 licenses to the U.S.S.R. and one each to the German Democratic Republic, Hungary, Poland and Romania for the export of technical data for foreign patent applications. See U.S. Department of Commerce, 120th Report on U.S. Export Controls to the President and the Congress (Semiannual: April 1979–September 1979), p. 14.

Others involved in export control policy, such as the Machinery and Allied Products Institute,[123] have envinced less certainty about the law and its implementing regulations. And where cryptologic equipment is concerned, so is the State Department's Office of Munitions Control.

7. INTERNATIONAL TRAFFIC IN ARMS REGULATIONS (ITAR)

Under the ITAR (see notes 7–15) and accompanying text), unclassified equipment on the U.S. Munitions List "shall not be exported from the United States until a license has been obtained from the Department of State, or it is otherwise exempt under other provisions of this subchapter."[124] As noted, the export of equipment performing cryptographic functions—including devices implementing the Data Encryption Standard (DES)—is subject to the ITAR.[124a]

An application to the Office of Munitions Control for an export license goes through a two-step evaluation process:

> First, a technical evaluation is made by the appropriate defense agency which, in the case of cryptography, is the National Security Agency. The Agency is given full information concerning the proposed transaction including the application and persons involved. Once the proposal has received agency approval, the Office of Munitions Control then reviews it for consistency with foreign policy objectives.[125]

---

[123] See generally the MAPI copyright study, U.S. Technology and Export Controls, Washington, D.C. (April 1978). "It is our understanding that over the years there have been only two instances of administrative action being taken with respect to violations of the Department of Commerce technical data regulations. Since both were settled through administrative procedures, there has not been a court test of the regulations" (note 1 at 10).

[124] 22 CFR 123.01 (1980).

[124a] At a National Bureau of Standards workshop on the DES, participant Walter Tuchman of IBM commented, "When we attempted to get the algorithm approved for export, we discovered that we had inadvertently utilized classified design principles. IBM has been requested by the National Security Agency not to divulge these principles." Report of the Workshop on Cryptography in Support of Computer Security, U.S. Department of Commerce, NBSIR 77–1291, p. 16 (Sept. 1977). The report also included responses to questions reflecting "several primary issues that were raised during the workshop. The responses have been prepared either by the staff af NBS or by the agency or authority responsible for the area concerned." The first was:

"Is it proper to have a standard based on classified design principles?

"There is no precedent for the Federal Government to publish unclassified standards in the area of cryptography. DES is the first government cryptographic standard that has been published for use outside the classified community. Design criteria for cryptographic systems which are developed by the government or intended for use by the government are always classified. Even though the DES algorithm was designed by a private organization for use in unclassified, non-government applications, the design criteria which overlap with classified design criteria will not be published by the government and the designers of the DES algorithm have agreed not to publish them. Evaluation methods and criteria will be treated similarly.

"The publication policy of unclassified standards in classified areas other than cryptography was not investigated. In general, design standards are not explicitly defined within the standard. On the other hand, performance standards do include a means of measuring compliance in the standard. The DES was developed as a design standard. A standard may be issued without specifying all the design criteria if it is useful, if competitors have an equal chance to utilize the standard and if it is explicit to the point that users and suppliers can adopt it" (Id. at 41).

[125] National Telecommunications and Information Administration memorandum (April 1980). Licenses may be denied, revoked, suspended, or amended by the State Department without prior notice whenever it believes "such action to be advisable in furtherance of (1) World peace; (2) The security of the United States: (3) The Foreign policy of the United States;" or whenever it believes that Sec. 38 of the Arms Export Control Act. 22 U.S.C. 2778, or this export regulation has been violated. 22 CFR 123.05 (1980). Some cryptographic equipment falls within Department of Commerce export jurisdiction and is multilaterally controlled to all destinations for national security reasons. These controls are established during multilateral negotiations with the International Coordinating Com-

(Continued)

The regulations also require licensing of the export of unclassified technical data, defined as:

> (a) Any unclassified information that can be used, or be adapted for use, in the design, production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance, or reconstruction of arms, ammunition and implements of war on the U.S. Munitions List; or (b) any technology which advances the state-of-the-art or establishes a new art in an area of significant military applicability in the United States.[126]

A footnote explains: "The initial burden of determining whether the technology in question advances the state-of-the-art or establishes a new art is upon the U.S. party or applicant in consultation with the cognizant agency of the U.S. armed forces."

The ITAR export controls over technical data

> shall apply whenever the information is to be exported by oral, visual, or documentary means. Therefore, an export occurs whenever technical data is inter alia, mailed or shipped outside the United States, carried by hand outside the United States, disclosed through visits abroad by American citizens (including briefings and symposia), and disclosed to foreign nationals in the United States (including plant visits and participation in briefings and symposia).[127]

Where patents are involved, an export license is required if the unclassified technical data "exceed the data used to support a domestic or foreign filing of a patent application."[128]

No export license is required if the unclassified technical data can meet the test of a general exemption. The first of these general exemptions is:

> (1) If it is in published form and subject to public dissemination by being:

(Continued)

mittee (COCOM) partners of the United States. Entry 1527A of the Commodity Control List reads:

"Cryptographic equipment and ancillary equipment (such as teleprinters, perforators, vocoders, visual display units) designed to ensure secrecy of communications (such as telegraphy, telephony, facsimile, video, data) or of stored information; their specialized components; and software controlling or performing the function of such cryptographic equipment. Also video systems which, for secrecy purposes, use digital techniques (conversion of an analog, i.e., video or facsimile, signal into a digital signal). (This item also covers digital computers and differential analyzers (incremental computers) designed or modified for, or combined with, any cipher machines, cryptographic equipment, devices or techniques including software, microprogram control (firmware) and/or specialized logic control (hardware), associated equipment therefor, and equipment or systems incorporating such computers or analyzers), except simple cryptographic devices or equipment only ensuring the privacy of communications, as follows:

(a) Equipment for voice transmission making use of fixed frequency inversions and/or fixed band scrambling techniques in which the transposition changes occur not more frequently than once every 10 seconds;

(b) Standard civil facsimile and video equipment designed to ensure the privacy of communications by an analog transmission using nonstandard practices for intended receivers only video system, equipment effecting the transposition of analog data);

(c) Video systems for pay television and similar restricted audience television, including industrial and commercial television equipment using other than standard commercial sweep systems.

A footnote advises, "Exporters requesting a validated license from the Department of Commerce must provide a statement from the Department of State, Office of Munitions Control, verifying that the equipment intended for export is under the licensing jurisdiction of the Department of Commerce." Export Administration Bulletin 206, pp. CCL–34, 35 (June 25, 1980).

[126] 22 CFR 125.01 (1980). Technical data also means classified equipment or information relating to items on the U.S. Munitions List. "Patent applications covered by a secrecy order fall in the same category as classified information " 22 CFR 125.02 (1980).

[127] 22 CFR 125.03 (1980).

[128] 22 CFR 125.04 (1980).

(i) Sold at newsstands and bookstores;

(ii) Available by subscription or purchase without restrictions to any person or available without cost to any person;

(iii) Granted second class mailing privileges by the U.S. Government; or,

(iv) Freely available at public libraries.[129]

The other general exemptions apply principally to information approved for public release by the Government and information directly related to previously approved export transactions.

The status of technical data under ITAR is summarized this way in a National Telecommunications and Information Administration contractor's document:

> Therefore, if the information is unclassified, once published domesticly it is no longer under the control of ITAR. The difficulty is that the act of publication domesticly could be interpreted as a violation of the regulation.[130]

At the subcommittee hearings, NSA Director Inman acknowledged troublesome ambiguities in the ITAR and testified that, as a result of NSA initiatives, the State Department's Office of Munitions Control had taken the matter under advisement and might issue a clarification "that will meet the concerns expressed by the scholarly community" (see note 77 and accompanying text). It was issued as Munitions Control Newsletter No. 80, dated February 1980, in response to concern that ITAR provisions relating to the export of technical data as applied to cryptologic equipment "can be so broadly interpreted as to restrict scientific exchanges of basic mathematical and engineering research data."

The Office of Munitions Control reported that, as it interprets the ITAR, cryptologic technical data for which a license is required includes

> in addition to engineering and design data, information designed or reasonably expected to be used to make such equipment more effective, such as encoding or enciphering techniques and systems, and communications or signal security techniques and guidelines, as well as other cryptographic and crytoanalytic methods and procedures. It does not include general mathematical, engineering or statistical information, not purporting to have or, reasonably expected to be given direct application to equipment in such categories. It does not include basic theoretical research data. It does, however, include algorithms and other procedures purporting to have advanced cryptologic application.[131]

The newsletter continued:

> The public is reminded that professional and academic presentations and informal discussions, as well as demonstra-

[129] 22 CFR 125.11 (1980). A footnote advises, "The burden for obtaining appropriate U.S. Government approval for the publication of technical data falling within the definition in Sec. 125.01, including such data as may be developed under other than U.S. Government contract, is on the person or company seeking publication."

[130] NTIA contractors memorandum (April 1980)

[131] Munitions Control Newsletter No. 80, signed by William B. Robinson, Director, Office of Munitions Control. Copies of the newsletter were distributed to members of the Public Cryptography Study Group in May. In Hearings.

> tions of equipment, constituting disclosure of technical data to foreign nationals, are prohibited without the prior approval of this office. Approval is not required for publication of data within the United States as described in Section 125.11(a)(1).[132]

It added that the cautionary footnote on otbaining Government approval for the publication of technical data (see note 129) "does not establish a prepublication review requirement."

The newsletter said the interpretation set forth "should exclude from the licensing provisions of the ITAR most basic scientific data and other theoretical research information, except for information intended or reasonably expected to have a direct cryptologic application," and added:

> Because of concerns expressed to this office that licensing procedures for proposed disclosures of cryptologic technical data contained in professional and academic papers and oral presentations could cause burdensome delays in exchanges with foreign scientists, this office will expedite consideration as to the application of ITAR to such disclosures. If requested, we will, on an expedited basis provide an opinion as to whether any proposed disclosure, for other than commercial purposes, of information relevant to cryptology, would require licensing under the ITAR.[133]

Whether this purported clarification has been received, understood and accepted by the scientific community cannot be gauged from the experience of the Office of Munitions Control. The office is "not aware of any significant comment" on the newsletter, and it has issued no licenses in 1980 for the export of cryptologic technical data.[134]

8. A NEW STRICTURE: MILITARILY CRITICAL TECHNOLOGIES

Section 5(d) of the Export Administration Act of 1979[135] declares:

> (2) The Secretary of Defense shall bear primary responsibility for developing a list of militarily critical technologies. In developing such list, primary emphasis shall be given to—
>
> (A) arrays of design and manufacturing know-how,
>
> (B) keystone manufacturing, inspection, and test equipment, and
>
> (C) goods accompanied by sophisticated operation, application, or maintenance know-how,
>
> which are not possessed by countries to which exports are controlled under this section and which, if exported, would permit a significant advance in a military system of any such country.

---

[132] Id. at 2.

[133] Id.

[134] Information from the Office of Munitions Control (Sept. 11, 1980). The newsletter was given its normal distribution to about 1,200 registered manufacturers and exporters. As noted above, members of the Public Cryptography Study Group were given the newsletter in May.

[135] Act of Sept. 29, 1979, Public Law 96–72, 93 Stat. 503. Sec. 5 is cited to 50 U.S.C. app. 2404.

> (3) The list referred to in paragraph (2) shall be sufficiently specific to guide the determinations of any official exercising export licensing responsibilities under this Act.
>
> (4) The initial version of the list referred to in paragraph (2) shall be completed and published in an appropriate form in the Federal Register not later than October 1, 1980.
>
> (5) The list of militarily critical technologies developed primarily by the Secretary of Defense pursuant to paragraph (2) to the provisions of subsections (c) of this section.

As of January 1980, considerable progress had been made in the definition of critical technology areas. The Department of Defense initially identified 15 such areas, and the Department of Energy separately specified 10 others. These 25 areas, plus intelligence community recommendations of additional areas for consideration, were presented in the report of the Critical Technology Implementation Interagency Task Group (CTIIG), as charged by Presidential Review Memorandum 31. After the CTIIG report was submitted, three critical technology areas were added to the list: nuclear-specific technology, chemicals and cryptography.[136]

Publication of the list in the Federal Register will reveal whether cryptography survived the winnowing process for criticality (the challenge of identifying, defining and narrowing the list was said to be a process of applying the criteria of military application, technical criticality and adversary capabilities).[137] Meanwhile, a Defense Department contractor has focused on the concerns which Defense Advanced Research Projects Agency (DARPA) officials

> have expressed about the need to prevent the transfer overseas of unclassified but militarily critical dual-use technologies information that has been or is being developed by U.S. academic researchers under DARPA contracts.[138]

The executive summary of the Betac Report declares:

> Our findings indicate that the Freedom of Information Act does add difficulties to the control of unclassified information related to the critical technologies produced under government contract with academic researchers and/or research centers. The FOI Act, however, is limited to information not controlled by other statutes. Thus, the Export

---

[136] See generally, "Final Report: Phase II of the United States Technology Transfer Export Controls Project." Betac Corporation, Arlington, Va. (January 1980). Jointly sponsored by the Office of the Under Secretary of Defense for Research and Engineering, the Office of International Security Affairs of the Department of Energy, and the Defense Advanced Projects Agency. Prepared under Contract No. MDA 903–C–0137 [hereinafter cited as "Betac Report"].

[137] Id. at 2. The DOD list published Oct. 1 did not include cryptography. However, the DOE list of energy-related militarily critical technologies published Oct. 1 included encryption technology in category IX (Safety, Security, and Survivability Technology). DOE explained: "Encryption technology is used for the concealment of information. It supports compaction of information to reduce transmission requirements. Encryption is also used to control identification or validation keys in many applications in which it is necessary for equipment to verify the identity of an individual or the validity of an order, before granting access to the individual or obeying the order. Knowledge of advanced encryption technology may both improve an adversary's capabilities in his own use of encryption, to our detriment, and enable him to penetrate our systems, gaining information, gaining access, or causing the execution of false commands." (45 FR 65167, October 1, 1980.)

[138] Id. at XV.

> Administration Act which subjects the export of all technical data relating to design, production, and/or manufacturing processes of items to various types of government regulation, is not overriden by FOI Act provisions. The EAA defines the export of technical data to include the release of this information to foreign nationals within U.S. academic institutions. It is our view, however, that this type of data dossemination can only be successfully controlled by the voluntary cooperation of American accademic researchers because strict enforcement EAA of (sic) provisions to academic institutions and academic researchers would be very difficult and could be counterproductive over the long term.
>
> In order to obtain the cooperation of academic researchers, it is suggested that methods be adopted to increase contractor's awareness of the problem and the potential significance of dissemination of critical technologies information to foreign nationals. These methods might include the use of informative circulars on critical technologies and the need for their control, or the addition of a new standard clause to DARPA contracts indicating that the contractor is aware of the provisions of the Export Administration Act as they pertain to the inappropriate release of technical data to foreign nationals. It is also suggested that contractors be informed that the failure of voluntary approaches to control of this information could result in tighter monitoring and enforcemnt of technical data export regulations.[139]

By express disclaimer, the views, conclusions and recommendations in the Betac Report are those of the corporation "and do not necessarily reflect those of the sponsors." They are noticed by this committee nonetheless. In the body of the report, the contractor elaborates on a possible new standard clause in DARPA contracts:

> Such a clause should require the contractor to acknowledge in writing that he is aware of the national security implications of the inappropriate dissemination of critical technology technical data and know-how. It should be explained to the contractors that the primary purpose of this clause would not be to make the contractor liable for any unauthorized export of such technical data (under the provisions of the Export Administration Regulations and the ITAR regulations (sic) he could anyway. The expressed purpose should be to guarantee that he has been informed of the need to exercise discretion in presenting such information in academic-related activities where this information might be obtained by foreign nationals, especially nationals of controlled nations.
>
> It should not be necessary to emphasize the fact that civil penalties exist for dissemination to unauthorized foreign nationals of technical data concerned with critical technologies. As noted earlier, to be successful, control of the dissemination of such data will require the voluntary coopera-

[139] Id.

> tion of the DARPA contractors. Attempts at setting up or strictly enforcing punitive regulations would alienate the academic community and would probably be unenforceable. When requesting cooperation from U.S. academic contractors DARPA could note that there are penalties under Federal law for failure to properly control export of this technical data, including dissemination in U.S. academic institutions, and that if voluntary efforts to limit dissemination are unsuccessful, stronger enforcement of existing export control regulations might have to be considered.[140]

The Betac Report thus contemplates adding restraint by contract to the Export Administration/ITAR arsenal. Researchers would be coaxed, cajoled or bullied into withholding unclassified technical data they might generate in critical technology areas (some of the other areas on the January 1980 list with cryptography were computer networks, telecommunications, vehicular engines, undersea systems and advanced seismic detection).

In its Chapter III overview, the Betac Report observes that exemption 4 of the Freedom of Information Act—which permits Federal agencies to withhold trade secrets and confidential business information—is applicable

> only when a government contract specifically requests that such information be withheld. In the case of information received from academic researchers, "intellectual property rights" to the work that they have done for the government usually remain with them. However, rather than wishing to have this information withheld from the public, academic researchers typically want to get it published and disseminated among their counterparts at other universities and research centers. The government cannot force them to request that such information be withheld from dissemination under FOI Act requests, although if a researcher were to voluntarily ask that information be withheld, there would not be any problem in withholding it under the law. Section C quoted above contains a detailed discussion of this problem.[141]

Thus, researchers would be induced—or, perhaps, coerced—into sacrificing their intellectual property rights in Government-supported work. At the same time, the Public Cryptography Study Group is trying to formalize a system of voluntary self-regulation in which, apparently all intellectual property rights in cryptographic research would escheat to the National Security Agency.

There are legislative threats as well. For example, the bill H.R. 7331, introduced on May 13, 1980, and referred to the Committee on Foreign Affairs, would amend the Arms Export Control Act to add the following section:

> "SEC. 38a. The Secretary of Defense, in consultation with the Secretary of State and the Secretary of Energy, is au-

---

[140] Id. at 75. This appears in Chapter III: "The Freedom of Information Act, Export Controls, and the Dissemination of U.S. Technical Information Prepared Under Government Contract."

[141] Id. at 69.

> thorized to prescribe regulations which specify information pertaining to items listed in the United States Munitions List that is required in the interests of the United States to be protected from disclosure in order to preclude the possibility of unauthorized export. Such regulations shall be published for public notice in the Federal Register. Notwithstanding any other provision of law, *information specified in such regulations, or materials revealing such information, shall not be published or disclosed unless the Secretary of Defense, in consultation with the Secretary of State and the Secretary of Energy, determines that withholding thereof is contrary to the national interest.*" (Emphasis added.)[142]

Under the bill, cryptographic information could be prohibited from publication or disclosure "to preclude the possibility of unauthorized export." This reductio ad absurdum of export control, far beyond any sort of licensing scheme, could bring about by law what the National Security Agency reportedly achieves by admonition, persuasion or appeal to patriotism—the prevention of publication.[143] It is the most drastic of the legislative proposals in the 96th Congress pertaining to cryptology.[144]

9. GOVERNMENT CRYPTOGRAPHIC POLICIES: UNDER THE LOOKING GLASS

> With the introduction of electronics to communications, codes which once consisted of written-letter substitution lists now involved special electronic circuitry to 'scramble' the

---

[142] On May 22 the bill was referred to the Subcommittee on International Security and Scientific Affairs. On June 2 executive comment on H.R. 7331 was requested from the Departments of State, Defense and Energy. No comments had been received as of Sept. 11, 1980. (The Committee on Government Operations notes that the Department of Commerce apparently was not asked for comment on H.R. 7331.)

[143] For example, in a letter of March 26, 1980, to the subcommittee chairman, Prof. Cipher A. Deavours of Kean College of New Jersey, an editor and founder of the journal "Cryptologia," wrote that in the 3-year existence of "Cryptologia" "there have been three occasions on which officials from the National Security Agency have caused, in one way or another, certain articles to be withheld from publication. The first of these involved an article on the cryptanalysis of the obsolete M–209 cipher machine by Robert Morris of Bell Labs here in New Jersey. Mr. Morris had submitted the article to us and it was accepted for publication. Evidently people from N.S.A. visited him and later he withdrew the article. On another occasion scientists at Sandia Labs were preparing an article on the distribution of certain types of prime numbers connected with the public key cryptosystem originated at M.I.T.—influence was put upon their superiors not to submit their work to us and their offer of submission was withdrawn." The third, he wrote, involved his own 100-page paper on Polish methods used to solve the German Enigma cipher machine before World War II. "I sent a copy of the article to N.S.A. to see if they wished any deletions. I asked for a reply in two weeks or so. About three months later, I got a call asking me not to publish the paper because 'it would hurt us'." (Letter in subcommittee files.) In a subsequent staff interview, Deavours said he did not want to inadvertently publish something inimical to the U.S. and was willing not to publish the Enigma paper, "but I wanted a decent reason." (April 10, 1980).

[144] In June 1980, the Department of Defense sent Congress a draft of legislation, "To amend title 10, United States Code, to add a new section to authorize the use of funds available to the Department of Defense for foreign cryptologic support." In a letter of transmittal, DOD General Counsel Togo D. West, Jr., explained: "Previously, the Secretary of Defense used the Emergency and Extraordinary Expenditure authority of the Appropriations Act to cover such payments. Since the requirement for these funds has been clearly identified and justified to the Appropriations Committees in the budget review process and is specifically dealt with in classified annexes to the Committees' repots (sic), funds for this purpose were removed from the Emergency and Extraordinary Expenditure category by the Appropriations Committees and a new category of foreign cryptologic support was added to the 1977 Appropriations Act. The Senate and House Appropriations Committees' conferees recommended at that time, and have continued to recommend, that permanent authorizing language be sought for this category of appropriations. The purpose of this legislation is to implement that congressional recommendation and provide permanent authorization of the category of foreign cryptologic support." (EC 4599 to the Speaker of the House, June 12, 1980.) The House Armed Services Committee reports that such legislation has not been introduced as of Sept. 12, 1980. (In July, the British magazine "New Statesman" accused NSA of using a secret telecommunications center in northern England to tap telephone and telex communications throughout Europe with the help of the British government. Washington Post, July 9, 1980, p. A14. See Hearings.)

> information content of a message before sending and 'descramble' it at the receiving end. Devices which perform this function have been developed to an extremely high level of sophistication by their respective government users to insure that equally sophisticated eavesdroppers who intercept the communications cannot, by computer analysis or other means, descramble the information. This scrambling or 'encryption' technology has become so critical that it is handled as a state secret by each respective using government.[145]

Presidential Directive/National Security Council–24, or PD–24, of November 16, 1977, set forth a national telecommunications protection policy and made the NSC Special Coordination Committee responsible for its implementation. It directed the Special Coordination Committee to exercise its responsibility through a Subcommittee on Telecommunications Protection chaired by the director, Office of Science and Technology Policy, with administrative support provided by the Secretary of Commerce.[146]

In February 1979, the White House issued a three-page statement of National Telecommunications Protection Policy that included these major elements:

> a. Government classified information relating to national defense and foreign relations shall be transmitted only by secure means.
>
> b. Unclassified information transmitted by and between government agencies and contractors that would be useful to an adversary should be protected.
>
> c. Nongovernmental information that would be useful to an adversary shall be identified and the private sector informed of the problem and encouraged to take appropriate measures.[147]

It announced these other management and policy review responsibilities:

> The Secretary of Defense shall act as the Executive Agent for Communications Security (COMSEC) to protect government-derived classified information and government-derived unclassified information which relates to national security. COMSEC is concerned with protective measures designed for the security of classified information and other information related to national security.[147a]

---

[145] John Metelski, "Telecommunications Privacy and the Information Society," 2 Telecommunications Policy 4 (December 1978), pp. 327–328. In Hearings.

[146] At the first meeting of the Subcommittee on Telecommunications Policy, "and to respond to a question of [NSA Director] Admiral Inman's on the relationship between cryptographic patents and First Amendment rights, it was determined that the Department of Justice should undertake an examination of the patent laws as they would apply to an individual's rights under the Amendment." Letter of March 19, 1980, from Christine Dodson, Staff Secretary, National Security Council, to the subcommitteechairman. (Letter in subcommittee files.)

[147] In Hearings. Examples of "nongovernmental information that would be useful to an adversary," given by NTIA Associate Administrator Donald Jansky, include the strategy to be used by American firms in negotiations against foreign competitors, changes in the prime interest rate, crop forecasts, the availability of critical materials, and developments in advanced technologies. (Cited in D. Kahn, "For. Affairs," *op. cit.* at 150).

[147a] A year earlier, EO 12036 on United States Intelligence Activities (issued Jan. 24, 1978) declared under "definitions" that communications security "means protective measures taken to deny unauthorized persons information derived from telecommunications of the United States Government related to national security and to ensure the authenticity of such telecommunications." 3 CFR 133 (1979 comp.). By contrast, the subsequent White House policy statement does not define the communications security domain to "telecommunications of the United States Government. (emphasis added)

> The Secretary of Commerce shall act as the Executive Agent for Communications Protection for government-derived unclassified information (excluding that relating to national security) and for dealing with the commercial and private sector (sic) to enhance their communications protection and privacy.
>
> It is recognized that there will be some overlap between the responsibilities of the Executive Agents, in that Defense will continue to provide some noncryptographic protection for government-derived unclassified information as it does now, and Commerce will have responsibilities in commercial application of cryptographic technology. The subcommittee will review such areas on a case-by-case basis and attempt to minimize any redundancies.[148]

In turn, the Secretary of Commerce appointed the National Telecommunications and Information Administration (NTIA) to carry out this presidential task. NTIA began collecting information on protection techniques, ranging from limited protection terminals for voice, data, facsimile and graphics, to bulk encrypted services, possibilities for avoiding vulnerable transmission routes, and PBX-oriented trunk protections, as well as potential network-oriented techniques.[149]

Cryptographic research is another activity of interest. An NTIA paper announced a study of the likely effect different national policies would have on the private sector:

> It will explore the likely effect of three government policies—highly restrictive, no change from the present, and no restrictions—on such factors as private-sector research investments, U.S. and foreign private-sector technological progress, and the U.S. share of world cryptographic equipment sales.[150]

At the subcommittee hearings, the witnesses from the Office of Legal Counsel of the Department of Justice, H. Miles Foy and Larry A. Hammond, discussed cryptographic research in the aftermath of the *Edler* case (see notes 12 and 14–15 and accompanying text), which pertained to blueprints and similar technical data used as a basis for producing military equipment. Mr. Foy testified:

> The constitutional issues have not disappeared if an attempt needs to be made to regulate the transmission of cryptographic ideas outside the *Edler* context. What Mr. Hammond was saying, in effect, was that the *Edler* decision has so narrowed the regulation, the criminal provision that makes the regulation enforceable, that we are still left with a problem that raises important constitutional issues.
>
> That is, how do you regulate the dissemination of important and dangerous, say, cryptographic information outside the *Edler* context? That is an issue that needs to be addressed.

---

[148] Id. at 3. One of the immediate technical actions announced was expansion of Executive Secure Voice Network (ESVN) systems. In his "Foreign Affairs" article, D. Kahn says this system "uses telephone scramblers—each about the size of two file drawers—to render conversations unintelligible to eavesdroppers." (*Op. cit.* at 150).

[149] D. Kraft and C. Wilk, "Emerging Federal Government Actions in Telecommunications Protections," NTIA (July 19, 1979).

[150] Id. at 4.

> It is an issue that is being addressed in the Executive Branch right now.[151]

In his Foreign Affairs article, "Cryptology Goes Public," David Kahn concluded:

> So cryptology, in 1945 a nation's most closely held secret, has gone public. But not even the procedures or forums for coming to grips with the new problems have been settled on. Their evolving substance will be harder still to resolve.[152]

10. REPRISE

At the hearings, appearing with author David Kahn and Prof. George Davida in a panel discussion of public cryptography, the director of the National Security Agency, Admiral B. R. Inman, characterized himself as "a novice in this area next to two experts," but said he had been a user of the product of the U.S. SIGINT (signals intelligence) system for 20 years, and added, "I came to this job in 1977 with a great appreciation for the value of the product of that system for national security." [153]

The discussion progressed to the question whether it is really possible even to attempt to police the dissemination of ideas and technology. Adm. Inman testified that "it would be indeed extraordinarily difficult to try to police ideas," and noted that, in his dialogue with the academic and business worlds, "we look to obviously voluntary participation and support by those who would be regulated." He then generalized:

> But as a new student to this whole process, I have found thus far in my examination that none of the ideas which have come forth in the public sector are in fact new. The Government has either directly or with some of its collaborators examined usually some years ago each of those that have come forth thus far.[154]

It would be virtually impossible for anyone to prove the negative proposition that none of the cryptographic ideas emanating from nongovernmental researchers was in fact new. Verifiable or not, *Inman* was contrasting the past and the future to suggest that concerted academic and industrial brainpower might produce quantum leaps in cryptographic applications in the next decade that would catch up to what the Government has already done.

While the committee cannot assess the relative intellectual standing of the NSA and the field of public cryptography, it can point to an episode in the Pentagon Papers case that press critic Ben H. Bagdikian commends "to those editors and publishers who continue to take at face value every portentous claim by government of dangerous thoughts and documents." In a copyright article about the

---

[151] In Hearings.

[152] Kahn, op. cit. at 159.

[153] To obtain foreign intelligence through the interception of telecommunications is known as "Signals Intelligence" (SIGINT), the NSA's dominant operational activity. It consists of "Communications Intelligence" (COMINT), or intelligence obtained through the interception of electronic signals (such as radar and missile emissions) which were not intended by the sender to communicate messages.

[154] In Hearings.

Progressive case,[155] Bagdikian recalls the Pentagon Papers case of June 1971, in which the Government made the claim that for the New York Times and the Washington Post to publish the papers—a classified study entitled "History of U.S. Decision-Making Process on Viet Nam Policy"—would cause grave, direct, immediate and irreparable harm to the United States that could result in the deaths of American military personnel.

In the Washington Post hearings, writes Bagdikian, the district and appeals court judges asked the Government to produce the "10 worst cases" of damage if the papers were published. The Government agreed, but said these cases were too sensitive to be heard in open court. They were even too sensitive to be heard in a closed courtroom and would have to be heard in the judge's chambers, with only the attorneys present. Bagdikian explains:

> Among other things, I was in charge of a crew researching the cases brought up by the government. In these cases, the government's "worst" presentations to the judges fell into one of three categories: Either the claimed secret document had already been released to the public by the government (the majority of cases), or it was information that was original reporting by the press with the clippings later classified by the military, or it was material issued publicly by Moscow, Peking or Hanoi and therefore already known to adversaries.
>
> Given that embarassment, the government, having reached the Court of Appeals, said it had another example so serious that once again it could be presented only to one judge and only in his chambers with only a selected few persons present.

Luckily, writes Bagdikian, the Post succeeded in getting one reporter—chief Pentagon correspondent George Wilson—admitted. On the appointed day the group was gathered around the desk of David Bazelon, chief judge of the U.S. Court of Appeals:

> A knock on the door announced the entry of an official courier. He carried a large leather briefcase shackled to his wrist. He placed the briefcase on Judge Bazelon's desk, unshackled and unlocked it, and withdrew a manila envelope. Judge Bazelon opened the manila envelope. Inside was a white envelope. Judge Bazelon opened the white envelope and pulled out yet another white envelope, this one sealed with wax and tied with a red ribbon. Judge Bazelon, a man not inexperienced in courtroom drama, gazed over his half-glasses at the red ribbon lying on his desk, sighed, and broke the seal on the last envelope.
>
> Inside was a top secret sensitive message from Vice Admiral Noel Gayler, director of the National Security Agency, the country's most secret intelligence operation, specializing in codes and interceptions. The admiral had sent under tight security the decoded text of a North Vietnamese order to its naval vessels in the Gulf of Tonkin in August of 1964. The same decoded text existed in the Pentagon Papers and this

[155] Bagdikian, "A Most Insidious Case," The Quill (June 1979). See Hearings. In the Pentagon Papers case. the Supreme Court agreed with district courts that the Government had not met the heavy burden of showing justification for imposition of prior restraint of expression. See *New York Times Co.* v. *United States,* 403 U.S. 713 (1971).

was the ultimate "worst case" of damage that would result if this decoded enemy message were published.

The government explained to Judge Bazelon that if this decoded message were made public it would jeopardize current military operations in Vietnam with consequent loss of American lives. And this would happen because publishing this text would inform the enemy that (1) we could intercept their most vital operational messages in combat, and (2) we could decode those messages.[156]

Post officials were appalled, Bagdikian relates, but reporter Wilson whispered, "I think I've seen that text somewhere else," and asked them to stall for time. Wilson opened a small green vinyl zippered bag and pulled out a volume of Senate Foreign Relations Committee hearings in 1968 on the origins of the Vietnam war.

Wilson looked through the Government Printing Office book, trying to find the place where he remembered having read those words before. He found it:

"It was exactly the document Admiral Gayler sent over and it was an official published document of the government. At the time, the government was eager to publicize the decoded message because they wanted to document their case that they had been attacked by the North Vietnamese in the Gulf of Tonkin and that the enemy had done it by cold calculation."

Wilson had the book shown to the judge. It may have been the single act, more than any other, that helped win the Pentagon Papers case, possible because there was a superb reporter who knew the system almost as well as the officials (and in this case, better).[157]

As the final point in this reprise, consider these views of Martin E. Hellman, Department of Electrical Engineering, Stanford University, on the national security-private sector tradeoff:

The real, although often unspoken, argument against extremely secure publicly available cryptosystems relates to government intelligence activities. If the public gets good encryption so will our foreign opponents and we will lose valuable sources of intelligence. While there is merit to this argument, there are other factors which must be considered.

It is only third world nations which do not possess secure cryptoequipment, and even this group of nations is patching their cryptographic leaks. The relative ease of building secure systems with current solid state technology and the availability of expertise in other nations makes the task of keeping secure systems from these nations an impossible one. Several years ago, David Kahn, author of *The Codebreakers*, estimated that NSA is only able to cryptanalyze 4 percent of the traffic it intercepts, and this percentage appears to be decreasing rapidly. There is thus only marginal value to National Security in keeping public encryption weak. When this is compared with the cost to the private sector of exposing all of our telecommunications to foreign powers or organized crime

[156] Id. at 26.
[157] Id.

spying operations, the benefits of public security are seen to greatly outweigh the cost to National Security.

I would go a step further and argue that it is in the interests of National Security for public encryption to be as secure as possible. The U.S. is the world's most computerized nation and is moving rapidly into electronic mail, electronic funds transfers, and other forms of communication that are particularly vulnerable unless portected cryptographically. We therefore stand to lose the most and gain the least by setting public encryption standards at a low level. The Soviets, by contrast, stand to gain the most and lose the least of all major powers.[158]

C. Recommendations

EXECUTIVE

1. The President:

a. Revise Executive Order 12065 on National Security Information by changing in paragraph 1–603 "proprietary interest" to "property interest," to make it agree with the Invention Secrecy Act. Delete or rewrite paragraph 1–205, the "Exceptional Cases" provision, as it creates the notion that classifiable information can arise spontaneously outside the classified community.

b. Report to the House Government Operations Committee on the results of Executive Branch discussions of public cryptography problems and prospects by March 1, 1981, and before adoption of a policy on public cryptography. At the hearings, the director of the National Security Agency and witnesses from the Justice Department referred to these discussions and their importance.

c. Dispel the confusion in White House directives and pronouncements over the meaning and responsibility for "communications security." On the one hand, Executive Order 12036 of Jan. 24, 1978, on U.S. intelligence activities declares that communications security means "protective measures taken to deny unauthorized persons information derived from telecommunications of the United States Government related to national security and to ensure the authenticity of such telecommunications." On the other hand, the White House statement of February 1979 on National Telecommunications Protection Policy says that communications security, or COMSEC, "is concerned with protective measures designed for the security of classified information and other information related to national security," neither confining the domain to "telecommunications of the United States Government" nor defining "national security."

2. Department of Justice:

a. Make public its memorandum opinions and any other studies of the relationship between cryptographic patents and First Amendment rights, and any others bearing on the classification of private ideas.

b. Should examine the various National Security Agency efforts to encourage private submission of research articles for pre-publication review—specifically, the draft proposal of the American Council of

[158] Hellman, "How Secure Should Commercial Encryption Be?" Draft manuscript (March 5, 1980), in subcommittee files.

Education's Public Crytography Study Group—and determine whether such efforts are within the NSA mandate and do not conflict with First Amendment requirements.

3. Department of State:

a. Review the U.SC. Munitions List and the International Traffic in Arms Regulations (ITAR) and report to the House Government Operations Committee on why the data encryption standard (DES) was placed and remains under the export control of ITAR. The DES algorithm was designed for use in unclassified and nongovernment applications, and has no obvious connection with the arms, ammunition or implements of war on the Munitions List. Also, determine whether "speech scrambers" and "privacy devices" indeed belong in the Auxiliary Military Equipment category of the Munitions List, or whether they can be deleted as neither exclusively nor primarily military items.

b. In light of the memorandum opinion of the Office of Legal Counsel of the Department of Justice in May 1978 on the constitutionality under the First Amendment of ITAR restrictions on public cryptography, review and rewrite the ITAR to satisfy constitutional objections.

4. National Science Foundation:

a. Repeat former NSF Director Richard Atkinson's 1978 suggestion that the National Security Agency begin a small, unclassified program ($2–3 million) of support for university research in public cryptography and renew its offer to loan expert personnel to NSA to help launch the program.

b. Whether or not the NSA undertakes such a small, unclassified program of support, the NSF should reject NSA efforts to involve itself in NSF's public cryptography programs on national security grounds.

5. National Security Agency:

a. Moderate its approach to the NSF over the national security implications of the latter's support of public cryptography.

b. Equip the Public Cryptography Study Group with the additional information its public members need to engage in a fully informed dialogue with the NSA over a possible system of voluntary self-regulation in crytographic research—including the memorandum opinion of the Office of Legal Counsel of the Department of Justice on the constitutionality of ITAR restrictions on public cryptography—and ask the sponsoring American Council on Education to extend the Group's life so that it can deliberate over the additional information. A copy of the Group's final report to the American Council on Education should be transmitted to the House Government Operations Committee at the same time that the report is forwarded to the Director of NSA.

c. Change its policy of, "The less published in public cryptography, the better," which leads it to tell private citizens and Government employees alike, "We'd rather you didn't publish this, but we can't tell you why." Authors often submit manuscripts to NSA for technical or policy review. By not making distinctions, the NSA risks exhausting their goodwill.

d. Adhere to the letter of the Invention Secrecy Act by conducting its national security review of patent applications so that the NSA director, not a subordinate acting in his behalf, determines that the Commissioner of Patents and Trademarks will be requested to issue a secrecy order. Leaving such decisionmaking to subordinates encourages bureaucratic mischance of the sort that led to a secrecy order for Prof. George Davida in April 1978.

III. ATOMIC ENERGY RESTRICTED DATA

A. Findings and Recommendations

In U.S. District Court in Milwaukee on September 4, 1980, a "final settlement" was reached in The Progressive magazine case in the form of a modified protective order that released about 95 percent of the briefs, affidavits and exhibits heretofore kept secret in the case. It brought to a nominal close a unique case in which the Government obtained a preliminary injunction on March 26, 1979, prohibiting The Progressive from publishing an article entitle, "The H-Bomb Secret: How We Got It—Why We're Telling It."

In the September 1980 court proceeding, U.S. District Judge Robert Warren said the Governor will not prosecute anyone for violations of the Atomic Energy Act in connection with the press freedoms case. He declined to award any costs in the case, meaning the defendants will have to pay their own legal expenses of about $250,000 incurred in fighting the first time ever prior restraint of publication. And he refused to remove from the record his orders which had prevented the Madison-based magazine from publishing the H-bomb article.

Now about 5 percent of the evidence in the case remains secret, most of it in a separate category created by Judge Warren's modified protective order which he calls "sensitive data." Judge Warren said the material will remain in that category for five years, and during that period, can be looked at but not quoted verbatim.

The documents released as a result of the "final settlement"— said to be a stack a foot high—most certainly contain a great deal of information relevant to this committee's fact-finding inquiry. However, as of the deadline for consideration of this report, more than two weeks after the September 4 court proceeding, the documents have not been received.

The delay in receipt of these documents from the Department of Justice presents a dilemma. The committee cannot make formal findings about *The Progressive* case without having examined and analyzed the newly available documents. They surely would flesh out an investigative record that was left incomplete because of the unwillingness of the Department of Justice and Energy to answer questions and supply information while *The Progressive* case remained in litigation.

At the same time, the committee compiled a thorough record of information and analysis about atomic secrecy, the background and oversight of the Atomic Energy Act, the development of the "born classified" concept with respect to atomic energy Restricted Data, the Department of Energy's use of invention secrecy orders, and the interlock between invention secrecy, Restricted Data and the national

security information classification system. It did so in the course of nine months of inquiry that included three days of subcommittee hearings, the commissioning of a study of the "born classified" concept by DOE Historian Richard Hewlett (now retired), the extensive assistance of the Congressional Research Service for studies and analyses, the receipt of written statements for the record from Government scientists and law professors on the facts of the court case and their relation to statutory and constitutional law, the availability of extensive files of correspondence offered by Congressman McCloskey and others, and numerous interviews and agency site visits by subcommittee staff.

Given this dilemma, the committee has decided to issue a report on atomic energy Restricted Data in the nature of a detailed discussion of the background, facts and problems, while withholding judgment about the finally settled *Progressive* case.

When the committee is able to complete its fact-finding record in *The Progressive* case, it will issue a follow-on report making findings and recommendations about the court case, the Atomic Energy Act and the ability of the Government to classify, restrict or assert ownership rights over privately generated information.

For now, the committee must content itself with the issuance of a report in the nature of a factual presentation, with its judgments and recommendations reserved. Much of the information contained in it is new and important. Combined with information about the court case that is yet to be received and analyzed, it will serve as the principal factual basis for the committee's forthcoming findings and recommendations.

B. Discussion

1. RESTRICTED DATA

A. Atomic Secrecy Background

German scientists working at the Kaiser Wilhelm Institute for Chemistry in Berlin discovered nuclear fission in late 1938. Word of the breakthrough spread quickly around the world. It pointed to the possibility of a chain reaction that could produce an explosive of unprecedented force. Writes William Sweet:

> A debate ensued among scientists as to whether they should continue to publish atomic research results, but initially there was strong resistance to the idea of secrecy among people whose work had depended for decades on the free exchange of information.

In April 1940, U.S. scientists agreed among themselves not to publish papers which might be of help to Germany, "and with the establishment of the Manhattan Project in August 1942, a tight system of government security was imposed on atomic weapons research." [1]

The atomic bomb project was one of the best kept secrets of the war. The day before the attack on Hiroshima in August 1945, most Americans had no idea that the Federal Government was developing the atomic bomb or that the Army Corps of Engineers had constructed

[1] Sweet. "Atomic Secrecy." Editorial Research Reports, Sept. 7, 1979 (Vol. II, No. 9), pp. 649–650.

a network of massive production plants and laboratories in a dozen States across the nation. Scarcely a score of civilian and military officials had formal access to the information generated in all parts of the Manhattan Project. Everything related to the project, including its very existence, was "born classified." [2]

In fact, a young Soviet psysicist, G. N. Flyorov, deduced from the "dogs that did not bark" that something was afoot and alerted Stalin. According to the historian David Holloway, Flyorov and a colleague had been cominated for a Stalin Prize for their discovery of the spontaneous fission of uranium, but the referee advised against the award, on grounds that foreign scientists were disinterested. Early in 1942, Flyorov looked at the foreign literature himself and confirmed that nothing on nuclear fission was being published in American or British journals. Writes Holloway:

> The names of Fermi, Szilard, Teller, Andersen, Wheeler, Wigner and others had disappeared from print. From the "dogs that did not bark" Flyorov deduced that nuclear research in the United States had now been made secret. American scientists had in fact decided in April 1940 to stop the publication of papers that might help Germany to develop the atomic bomb. They thus unwittingly alerted Soviet scientists to American work on the bomb.
>
> Flyorov now decided to take his case to the very top. In a letter to Stalin he explained the nature of the uranium problem in both its military and its peaceful aspects. He pointed to the secrecy of research in America and called for the immediate reestablishment of a nuclear laboratory. "It is essential," he wrote, "not to lose any time in building the uranium bomb." [3]

In October 1942, nuclear physicist Igor Vasil'evich Kurchatov agreed to head up a Soviet atomic bomb project.

In the weeks following the Hiroshima and Nagasaki raids, a general description of the organization and scientific principles used to produce the bomb did become public, but every technical specification of the process employed remained classified, including even the fundamental physical properties of the heavy elements.[4] On August 6, 1945, Secretary of War Henry L. Stimson explained:

> It was early recognized that in order to make certain that this tremendous weapno would not fall into the hands of the enemy prompt action should be taken to control patents in the field and to secure control over the ore which is indispensable to the process. Substantial patent control has been accomplished in the United States, the United Kingdom, and Canada. In each country all personnel engaged in the work, both scientific and industrial, are required to assign their

---

[2] Hewlett, Richard G. The "Born-Classified" Concept in the U.S. Atomic Energy Commission. An Historical Study prepared for the Subcommittee on Government Information and Individual Rights of the House Committee on Government Operations by the Chief Historian, Department of Energy, May 1980 (see appendix to this report) [hereinafter cited as "Hewlett born-classified study"].

[3] Holloway, "Entering the Nuclear Arms Race: The Soviet Decision to Build the Atomic Bomb, 1939–45." Working Paper No. 9, International Security Studies Program, The Woodrow Wilson International Center for Scholars, Washington, D.C., 1979.

[4] Hewlett, Op. Cit.

entire rights to any invention in this field to their respective governments. . . . All patent actions taken are surrounded by all safeguards necessary for the security of the project.[5] . . .

In the period November 1944–December 1946, 25 patent applications covering Manhattan Project inventions were filed in the Patent Office and assigned serial numbers, but not deposited there. Under special arrangement, the applications were sealed in individual packages and retained for safekeeping by the wartime Office of Scientific Research and Development and its sucessor, the Atomic Energy Commission.

On September 14, 1950, the application files, in sealed packages, were hand-carried by AEC officials to the Patent Office for inspection and addition of power-of-attorney and other papers. The files were opened, examined, repckaged, seled before witnesses and handed back into AEC custody by Patent Commissioner John A. Marzall.

In January 1979, the Department of Energy undertook a classification review of the files corresponding to those in the sealed packages. As a result, 17 of the applications were deemed to be Secret Restricted Data, and the remaining eight were classified Restricted Data. On June 7, the 25 sealed applications were returned to the Patent Office and, in the presence of witnesses, inspected for evidence of tampering. Donald W. Banner, Commissioner of Patents and Trademarks, compared the seals with the one used to close each envelope in 1950. Then the seals were broken and the applications were reexamined for verification. Commissioner Banner acknowledged receipt of the 25 applications which had been kept in special hiding for nearly 35 years.

In a subsequent letter, DOE expressly abandoned each of the 25 Manhattan Project patent applications, since these weapons inventions are regarded as unpatentable under the Atomic Energy Act of 1954. However, information about them continues in secret repose as atomic energy Restricted Data.[6]

B. The Atomic Energy Act: 1946 and 1954[7]

In drafting proposed legislation for the postwar control of atomic energy and in administering the laboratories in the Manhattan Project, the War Department gave indications that the very rigid controls over scientific activities might be continued into the postwar period. Many of the nation's most prominent nuclear scientists spoke out against continued controls over basic research. Enrico Fermi remarked, "Unless research is free and outside of control, the United States will lose its superiority in scientific pursuit."

Concern for scientific freedom dominated the first draft of the atomic energy bill introduced by Senator Brien McMahon on December 20, 1945. In its statement of purposes, the bill gave greatest emphasis to "fostering private research and development on a truly independent basis" and to "free dissemination of basic scientific information and for maximum liberality in dissemination of related technical

[5] Quoted in "Federal Information Controls In Peacetime," compiled by Robert E. Summers. The H. W. Wilson Company, New York (1949).

[6] From "Memorandum For The File—'Item 25'," by C. D. Quarforth, Director, Group 220, Patent and Trademark Office, and a general history of the handling of these applications prepared at subcommittee request by Anthony Campana, Technical Adviser, Office of the Assistant General Counsel for Patents, DOE. See Hearings.

[7] Principal authorities for this narrative section are Hewlett, Op. Cit., and Kent M. Ronhovde, American Law Division, Congresssional Research Service, Library of Congress, fn legislative histories of select secrecy provisions of the Atomic Energy Act of 1946 and the Atomic Energy Act of 1954.

information." Section 9 of the bill, entitled "Dissemination of Information," attempted to distinguish between scientific and related technical information by declaring that basic scientific data "shall include in addition to theoretical knowledge of nuclear and other physics, chemistry, biology, and therapy, all results capable of accomplishment, as distinguished from the processes or techniques of accomplishing them." The latter would fall in the category of "related technical information." Under the bill, the new Atomic Energy Commission would be authorized to restrict the dissemination of technical information in the interest of national security "within the meaning of the Espionage Act."

In almost four months of hearings and executive sessions on the bill, McMahon's Special Committee on Atomic Energy moved toward a more conservative position on the dissemination of scientific and technical information than the scientists advocated. What may have been a predeliction was reinforced by revelations in January and February 1946 of Soviet espionage activities on atomic energy projects in the United States and Canada. The committee also was concerned about practical matters, such as the inadequacy of the Espionage Act to protect sensitive technical information.

The Committee's revisions of the bill in April 1946 reflected greater reliance on security. The declaration of policy in Section 1(a) was amended to read:

> Accordingly, it is hereby declared to be the policy of the people of the United States that, *subject at all times to the paramount objective of assuring the common defense and security*, the development and utilization of atomic energy shall, *so far as practicable*, be directed toward improving the public welfare, increasing the standard of living, strengthening free competition in private enterprise, and promoting world peace. (portions in italic were added to original bill)

In the same vein, the title of section 9 (now Section 10) was changed from "Dissemination of Information" to "Control of Information."

The committee also abandoned the attempt to distinguish between "basic scientific" and "related technical" information, and deleted the declaration establishing free dissemination as the cardinal principle in information policy. In place of the distinction between "scientific" and "related technical" information, the committee decided to establish a special category of classified information to be called "Restricted Data," to be defined as

> all data concerning the manufacture or utilization of atomic weapons, the production of fissionable material, or the use of fissionable material in the production of power, but shall not include any data which the Commission from time to time determines may be published without adversely affecting the common defense and security.

The definition acknowledged the existing situation—that all information related to these aspects of nuclear technology was already classified and could be declassified only by positive action on the AEC's part.

Yet Senate Report 1211 of the 79th Congress, 2d Session, summarizing the findings of the special committee, said about the problem of secrecy:

> The secrets which we hold are matters of science and engineering that other nations can and will discover. In large part they are secrets of nature, and the book of nature is open to careful, painstaking readers the world over. We can give ourselves a certain temporary protection by retaining the secrets we now have. But that protection grows weaker day by day, and our research must be vigorously encouraged, supported, and pursued if we are to maintain our place among other nations, to say nothing of retaining our advantage.

The bill passed the Senate on June 1. It was subsequently reported out by the House Committee on Military Affairs with amendments that did not significantly affect the "control of information" provisions, the patent sections or the compensation language, but the report contained minority views disagreeing with the patent visi. After lengthy debate and amendment on the floor, the bill passed the House on July 20.

In conference, the House receded from its amendment making major changes in the bill's patent provisions, but the control of information and "compensation for private property acquired" sections were not significantlly altered. The bill was signed by the President on August 1.

The sense of Congress was far more on the side of tight control of atomic energy information than on the side of Liberal dissemination. Atomic energy was a frightening, mysterious force to be locked away behind the security barriers of the Government project. In 1946 it had no place in the everyday life of most Americans.

Without ever using the term, the Atomic Energy Commission adopted the "born classified" concept as a working assumption. Given the act's definition of Restricted Data, everything encompassed by it was automatically classified. This meant that virtually every one of the hundreds of thousands of documents generated in the wartime project would have to be reviewed before it could be declassified.

By 1953, pressures from private industry for access to nuclear technology, particularly on reactor development, had produced a climate for revision of the act. On February 17, 1954, President Eisenhower recommended amending the Atomic Energy Act of 1946 "for the purpose of strengthening the defense and economy of the United States and the free world." His message to Congress stated:

> These amendments would accomplish this purpose, with proper security safeguards, through the following means:
>
> First, widened cooperation with our allies in certain atomic energy matters;
>
> Second, improved procedures for the control and dissemination of atomic energy information; and,
>
> Third, encouragement of broadened participation in the development of peacetime uses of atomic energy in the United States.

The message added that

> [m]any statutory restrictions, based on such actual facts of 1946 as the American monopoly of atomic weapons and limited application of atomic energy in civilian and military fields, are inconsistent with the nuclear realities of 1954. Furthermore, these restrictions impede the proper exploitation of nuclear energy for the benefit of the American people and of our friends throughout the free world.

It also discussed in detail proposals for the protection of atomic energy information and the need to encourage domestic development of this energy form.

Following submission of the President's message, the Joint Committee on Atomic Energy drafted a series of amendments to the act. Eventually these became an entirely new statute, the Atomic Energy Act of 1954, although the portions of the earlier act dealing with Restricted Data and information control emerged essentially unchanged. The new act did provide that private industry could have access to Restricted Data in specific categories if it agreed to comply with AEC regulations on classification and security.

Identical reports were filed in the House and Senate (H. Rept. No. 2181 and S. Rept. No. 1699, 83rd Cong., 2d Sess., 1954) on the bills incorporating the amendments to the 1946 act. In analyzing the pertinent sections, the report stated:

> CHAPTER 12 CONTROL OF INFORMATION
>
> This chapter sets forth provisions for the protection of secret information relating to atomic energy.
>
> Section 141 sets forth the policies for dealing with restricted data; namely, that the Commission shall control the dissemination and classification of restricted data in such a manner as to assure the common defense and security; that the exchange of restricted data with other nations before enforcible international safeguards against the use of atomic energy for destructive purposes have been established are forbidden except pursuant to agreements for cooperation under section 144; and that dissemination of technical information is to be encouraged so as to have the free interchange of ideas and criticism which is essential to scientific and industrial progress and public understanding and to enlarge the fund of technical information.
>
> Section 142 directs the Commission to declassify that information within the definition of restricted data that can be published without undue risk to the common defense and security. It also directs the Commission to make continuous reviews of restricted data and of the classification guides so as to determine which information can be so declassified and published. That restricted data which the Commission and the Department of Defense jointly agree relate primarily to the utilization of atomic weapons, and which they jointly determine can be published without undue risk to the common defense and security, can be removed from the classification

of restricted data. The President is authorized to settle any disputes respecting such determinations. In addition, the Commission with the concurrence of the Department of Defense, can remove from the category of restricted data any information which they jointly determine relate primarily to the utilization of atomic weapons and which they determine can be adequately protected as defense information. However, any restricted data so classified as defense information cannot be transferred to any other nation except pursuant to an agreement for cooperation in accordance with subsection 144 b. The Commission is also authorized to remove from the category of restricted data any information relating to the atomic-energy programs of other nations that the Commission and the Director of Central Intelligence jointly determine to be necessary to carry out the provisions of section 102 d. of the National Security Act of 1947.

Section 143 authorizes the Commission to permit those in its program to provide access to restricted data to persons associated with the Department of Defense, where such access is required in the performance of the duties of the person to whom such access is to be granted, and the head of the agency or department in the Department of Defense so certifies. Furthermore, the head of that agency in the Department of Defense must certify that it has been established in accordance with the usual procedures of that agency that permitting such person to have the access permitted will not endanger the common defense and security, and the Secretary of Defense must find that the security procedures are adequate and in reasonable conformity with the standards established by the Commission.

Section 144 permits the President to authorize the Commission, pursuant to agreements for cooperation, to communicate certain types of restricted data which relate to the nonmilitary aspects of atomic energy to other nations. (The specific fields are described in the discussion of sec. 123 above.) This section also permits the President to authorize the Department of Defense to cooperate with another nation or with a regional defense organization, pursuant to an agreement for cooperation and to disclose certain limited types of restricted data relating to the use of atomic weapons. (The specific areas of disclosure permitted are also set forth in the discussion of sec. 123 above.) This section also requires that the other nation or regional defense organization participate with the United States pursuant to an international arrangement by making substantial and material contributions to the mutual defense and security.

Section 145 requires personnel investigations by the Federal Bureau of Investigation or by the Civil Service Commission of persons who will be employed by the Commission or given access to restricted data. It permits the Commission or the General Manager (and this permission rests solely with those named) to exempt persons from this requirement where such exemption is clearly consistent with the national inter-

est. The Federal Bureau of Investigation is required to handle any cases in which the Civil Service Commission finds any information which indicated questionable loyalty. It is also required to conduct investigations for those groups or classes of persons specified by the President, or for those positions certified by the Commission to have a high degree of importance of sensitivity. The Commission is authorized to establish the scope and extent of the less sensitive investigations permitted to be conducted by the Civil Service Commission, depending upon the degree of importance to the common defense and security of the restricted data to which access will be permitted.

Section 146 continues the application to restricted data and to persons in the atomic energy program of other laws relating to the protection of information. It also forbids the Commission from controlling or restricting any information outside of any powers granted by any law.

CHAPTER 13. PATENTS AND INVENTIONS

This chapter sets forth the provisions under which patents may be issued, and used in the atomic energy field.

Section 151 forbids the issuance of any patent on an invention or discovery useful solely in the utilization of atomic energy or of special nuclear material in an atomic weapon. Where inventions or discoveries have uses other than in weapons, patent rights are forbidden to the extent that the fields set forth above are involved. Any person making any invention or discovery generally useful in the field of atomic energy, is required to report that invention or discovery to the Commission, or to file a patent application on it within 90 days. The Commissioner of Patents is required to keep the Commission fully informed of all applications in the field of atomic energy. These latter provisions are to keep the Commission fully and currently aware of all technology in the field of atomic energy.

Section 152 permits the Commission to find that a patent is of primary importance in the production or utilization of special nuclear material or atomic energy, and that the licensing of the invention is of primary importance to effectuate the policies and purposes of the act. Upon making such a finding, the Commission may declare the patent to be affected with the public interest. Thereafter the Commission itself is licensed to use the invention, and other persons engaged in activities authorized by the bill may apply to the Commission for and may be granted a patent license to use the patent if the Commission finds that such a patent license is of primary importance to the conduct of such activities.

The bill also authorizes any person engaged in an atomic energy activity authorized by the bill to apply to the Commission for a license on a patent which has not been declared to be affected with the public interest. In such cases, the Commission is required to grant a patent license to such person

after hearing all materially interested parties, if the Commission finds (1) that the idea or invention involved is of primary importance in the production or utilization of special nuclear material or atomic energy; (2) that the licensing of such patent is of primary importance to the activities of the applicant; (3) that the activities to which the patent license is to be applied are of primary importance to the furtherance of the policies of the bill; and (4) that the applicant cannot obtain a patent license from the owner of the patent on terms which the Commission deems reasonable. The Commission is required to see that the owner of any patent declared to be affected with the public interest, or licensed by this section, receives a reasonable royalty fee for any such use of the patent.

Section 153 provides that no injunction may be issued against the holder of a patent license issued under the provisions of section 152 and that in any court action brought against such a patent licensee, the action is to be stayed until the royalty is determined pursuant to those provisions of this bill.

Section 154 provides that no patent may be issued on an invention or discovery known before in this country even though such invention has been known or used in the atomic program in secret.

Section 155 requires the Commission to establish standard specifications for the issuing of any patent license for any patent held by the Commission.

Section 156 establishes a Patent Compensation Advisory Board to consider applications under this chapter. The members are to be paid a per diem and may serve without regard to the conflict of interest statutes except as atomic energy matters may be involved. The Board may hear applications from the owners of a patent licensed under the compulsory licensing provisions or from the owners or persons seeking to obtain just compensation for patent rights eliminated by the statute and may also hear applications for awards by persons who have made any invention or discovery not otherwise entitled to compensation or royalty. The Commission is permitted, upon the recommendation of the General Advisory Committee and with the approval of the President, to grant an award for any especially meritorious contribution to the development, use or control of atomic energy.

In determining the reasonable royalty to be paid, the Commission is required to consider the advice of the Patent Compensation Advisory Board, any defense which might be pleaded in an action for infringement, the extent of any Federal financing involved, and the degree of utility, novelty, or importance of the invention, and may consider the cost of developing or acquiring the patent. In determining just compensation and awards, the Commission is required to consider the extent of actual use of the invention or discovery as well as those considerations involved in royalty determinations.

Section 157 declares that the Commission may continue to

require that patents made or conceived during the course of federally financed research or operation be assigned to the United States.

Section 158 permits any person who had applied for a patent which was earlier prohibited by the act, and which would now be permitted by the bill, to reinstate his application for the patent. No patent so reinstated can form the basis of a claim against the United States.

CHAPTER 15. COMPENSATION FOR PRIVATE PROPERTY ACQUIRED

This chapter establishes the rules for acquiring property condemned and used for public purposes.

Section 171 requires that, where the United States takes any interest in property for which just compensation is required to be paid under the terms of this bill, the Commission shall determine and pay such just compensation except in the case of real property. If that determination is not satisfactory, the Commission is required to pay 75 percent of the amount and the claimant is entitled to sue in the Court of Claims, or in the district court for the district in which he resides, for such further sum as added to the 75 percent will continue just compensation.

Section 172 requires that real property shall be condemned pursuant to the normal condemnation statutes and procedures.

Section 173 requires the Commission to pay just compensation for the disclosure of restricted data to any foreign nation where such restricted data is based on a patent application owned by a person other than the United States. If the claimant does not believe the Commission's determination of the amount to be just compensation is a proper amount, the Commission is required to pay 75 percent of the amount, and the claimant can sue for such further sum as added to the 75 percent will constitute just compensation.

Section 174 requires the Commission to receive the approval of the Attorney General on the title of any real property to be occupied, used, or improved by the Commission except where the President determines that prior approval of the title by the Attorney General is not required in the interest of the common defense and security.

CHAPTER 18. ENFORCEMENT

This chapter establishes the provisions for enforcing the bill.

Section 221 permits the President to utilize the services of any Government agency to protect the property of the Commission or to prevent the unlawful dissemination of restricted data. The Federal Bureau of Investigation is required to investigate all alleged or suspected criminal violations of the bill. No action maybe brought for any violation of the act until the Attorney General has advised the Commission with respect to such action. All actions are required to be brought

by the Attorney General as the legal representative of the Commission before the courts. In those cases involving the death penalty, action may be brought only on the express direction of the Attorney General himself.

Section 222 establishes criminal penalties for violation of certain of the prohibition sections within the act. The maximum penalty, if the offense is committeed with intent to injure the United States or with intent to secure an advantage to any foreign nation, is, on recommendation of the jury, death or imprisonment for life.

Section 223 establishes the criminal penalties for violation of all of the balance of the provisions of the act or for rules and regulations issued under certain specified limited statutory authority. There are lesser penalties attached to this section, through the maximum penalty, if the offense is committed with intent to injure the United States or with intent to secure an advantage to any foreign nation, is, $20,000 or 20 years or both.

Section 224 establishes the penalties for the disclosure of restricted data with intent to injure the United States or with intent to secure an advantage to a foreign nation. The maximum penalty is, on recommendation of the jury, death or imprisonment for life.

Section 225 establishes criminal penalties for acquiring restricted data with intent to injure the United States or with intent to secure advantage to any foreign nation. The maximum penalty is, on recommendation of the jury, death or imprisonment for life.

Section 226 establishes criminal penalties for altering or changing any restricted data with intent to injure the United States or with intent to secure an advantage to any foreign nation. The maximum penalty is, on recommendation of the jury, death or imprisonment for life.

Section 227 prohibits any person authorized to have restricted data from knowingly communicating, or whoever conspires to communicate or to receive, restricted data to any person known not to be authorized to receive restricted data, knowing that the information communicated is restricted data. The penalty is a fine of $2,500.

Section 228 establishes a 10-year period of limitation for noncapital offenses described in sections 224, 225, and 226.

Section 229 continues the applicability of any other laws (including the espionage law) to the field of atomic energy.

Section 230 permits the Attorney General to petition a court on behalf of the Commission for the injunction of any act which the Commission believes will violate any provision of the bill.

Section 231 permits the Attorney General to petition a court for an order requiring any witness to obey a subpoena served upon the witness by the Commission or to obtain an order of the court punishing the witness for contempt in the event the order is disobeyed.

After lengthy debate and amendment, H.R. 9757 passed the House on July 26, 1954. The Senate also held long floor discussion, finally passing its version of H.R. 9757 in lieu of S. 3690 the following day. A conference report reconciling differences in the two bills was filed August 6 and adopted by voice vote of the House but rejected by the Senate. A second conference report was filed and agreed to in each House. The measure was signed by the President on August 30, 1954, becoming Public Law 703.

The provisions of the Atomic Energy Act of 1954 that pertain to secrecy will be discussed below in the context of the *Progressive Magazine* case. Meanwhile, the "born classified" concept, sired by the absolute secrecy of the Manhattan Project, became a foundling of the Atomic Energy Commission.

C. The "Born Classified" Concept [8]

Without ever using the term, the AEC adopted the "born classified" concept as a working assumption. From 1946 to 1960, the Commission and its staff juggled two conflicting policy objectives set down in the 1946 act: to protect the common defense and security, on the one hand, by retaining as Restricted Data any information that might jeopardize the nation's monopoly of nuclear technology and the bomb, and, on the other, to declassify as much basic scientific information as possible and encourage scientific research on atomic energy.

The Commission realized when it took over the wartime project from the Army in January 1947 that hundreds of thousands of documents would have to be reviewed before they could be declassified. It was more than a year before any substantial amount of information was removed from the Restricted Data category and made available to the public.

Initially, it assigned classification officers at each major site to consider declassification requests as they arose and established a committee of Senior Responsible Reviewers to assure some uniformity in their decisions. Under prodding by laboratory scientists, the Commission cautiously opened a few topics to unclassified investigation: radiation instruments, particle accelerators, specific chemical processes, and medical research and health studies.

Under further prodding by scientists, the AEC in August 1948 lifted restrictions on all instrumentation, mathematics and all aspects of research in the physical and biological sciences which did not involve the fission process, weapons, or the properties or characteristics of elements above atomic number 90. This restriction effectively prohibited unclassified work on uranium or plutonium or on the development of nuclear reactors.

As of 1954, a limited number of AEC contractors had for many years had access to Restricted Data, but the Commission imposed its security and classification regulations on the companies by contract. By doing so it avoided the troubling problem of the private generation of Restricted Data. Indeed, all Restricted Data born classified in the 1950's was kept under Commission control.

[8] Principal authorities for this narrative section are Hewlett, *Op. Cit.*, and Suzanne Cavanagh, Government Division, Congressional Research Service, Library of Congress, in Congressional Discussion of the "Born Classified" Concept of the Restricted Data Clauses of the Atomic Energy Acts of 1946 and 1954, a report for the Subcommittee on Government Information and Individual Rights of the House Committee on Government Operations (July 22, 1980).

However, the AEC's legal staff was aware of the potential problem. In the summer of 1947, the scope of the act's Restricted Data section had been discussed with the Department of Justice. In a formal letter to the Commission, the Attorney General addressed what he called "the problem of censorship of 'off-project' development." He wrote there was "considerable indication" that Congress intended the section "to cover all aspects of atomic development, whether under government sponsorship or otherwise, and to prohibit the dissemination of information relating to any such activities."

The Attorney General admitted, nonetheless, that application of the section to private activities was "not lacking in difficulties, and that all areas of doubt on the part of laymen could be removed by amending it," perhaps by adding the words "whatever the source or origin" of the information. The Commission sent his letter to the Joint Committee on Atomic Energy, but no further action was taken.

Not until 1953, when private industry was urging the Federal Government to relax its monopoly on atomic energy technology, did the "born classified" concept come under consideration and criticism in hearings of the Joint Committee. In prepared testimony before the Joint Committee, J. G. Beckerly, the AEC's Director of Classification, commented on security considerations, the "born classified" concept and the need for declassification of certain atomic energy information:

> The basis for secrecy in atomic energy matters stems from the Atomic Energy Act itself. Under section 10 of the act power reactor information is 'born' classified and remains in this state until the Commission determines that the information, in the words of the statute, 'may be published without adversely affecting the common defense and security.' The reason reactor data has security implications lies in the fact that nuclear reactors are capable of producing fissionable material for atomic weapons. A second reason that reactor data may be security information is the fact that nuclear fuels may be used for military propulsion purposes. Reactor information also may have security significance because of its relationship to fissionable materials production capacity. The latter is clearly an intelligence factor whereas the first two concerns technical use of the data by unfriendly nations in their own programs.
>
> It is clear that the Commission must release at least as much reactor data as other nations have developed and published. This means that as other nations develop nuclear reactors and publish data thereon, it is pointless to withhold from publication similar data developed in this country. This is, of course, a minimum declassification requirement.
>
> Although we shall continue to withhold the critical details of reactor core technology, it is essential that we declassify more and more information on what can be done in a reactor core without divulging precisely how it can be done. This means, for example, that we should find it possible to discuss engineering evaluation on core performance; that is, degree

of burn up, lifetime of fuel elements, corrosion resistance, et cetera.[9]

In presenting the view of a Special Committee on Atomic Energy of the Association of the Bar of New York, its chairman, Oscar M. Ruebhausen, called for a public debate on atomic energy matters:

> I would like to make three observations.
>
> First, I believe the time has come for a full reexamination of the Atomic Energy Act of 1946, of the assumptions to which it gave expression, and of the policies which it put into effect.
>
> Second, I believe that the secrecy complex has wrongly dominated the national approach to atomic problems, that secrecy—which is a negative policy at best—has been mistakenly relied upon to achieve affirmative objectives, and that the role of secrecy in atomic matters should, in the imperative national interest, be reduced.
>
> Third, I believe that the reasons which led to the establishment of a Government atomic monopoly in 1946 are no longer compelling and that those provisions of the law which created that monopoly should be amended.[10]

In response to questions, Ruebhausen asserted that secrecy impeded this nation's development of an atomic energy industry:

> Now, a word about secrecy. Secrecy in government is the very antithesis of democracy. The basic tenet of our democracy is, as Judge Learned Hand has said, that "the right conclusions are more likely to be gathered out of a multitude of tongues than through any kind of authoritative selection." This is the principle on which we have staked our all as a nation—yet it is a principle from which we have departed in the case of nuclear fission.
>
> In the name of security we have fenced off and marked "For the AEC only" an entire science, a wholly new industry, and a large and steadily expanding Government operation. We would not have dreamed of indulging in such a fundamental departure from principle for anything other than nuclear physics. We don't do it for electronics, or for chemistry, or for the aircraft industry. Yet each of them is an inextricably involved in our security as is the atom. Why then have we done this to the atom? Atomic secrecy is, I think, the special price we are paying for the fright and the shock with which the phenomenon of fission clouded our thinking in 1945. The price is exhorbitant because it subordinates a fundamental principle of democracy to a concept of temporary military expediency.[11]

In his closing remarks, Ruebhausen addressed the concept of "born classified," and urged its reversal:

---

[9] U.S. Congress. Joint Committee on Atomic Energy. Atomic Power Development and Private Enterprise. Hearings, 83d Cong., 1st Sess., June 24, 25, and 29; July 1, 6, 9, 13, 16, 20, 22, 23, 27, and 31, 1953. Washington U.S. Govt. Print. Off., 1953. p. 36, 38.

[10] Id. at 471.

[11] Id. at 472–473.

> But there is one specific suggestion I would like to make. Under the present law the conception of secret, or restricted, atomic data is extremely broad. It includes not only military data but also all data concerning the production of fissionable material and, indeed, the use of fissionable material in the production of power. Today, in effect, all data in the atomic field is 'born secret'—and it stays secret until the Commission can meet the almost impossible burden of proving that its release will not adversely affect the common defense and security.
>
> I think it clear that this approach should be reversed. I would urge that the law be revised so that all atomic data will be "born free," as it were, except for data falling within certain specific categories defined by the Congress—such as data related to the manufacture or use of atomic weapons—and except for data which the AEC affirmatively determines cannot be published without adversely affecting the common defense and security. Under such a proposal data concerning the use of fissionable material in the production of power, for example, would become public unless the AEC found positive reasons for holding it secret.[12]

In 1956, the Panel on the Peaceful Uses of Atomic Energy, chaired by Robert M. McKinney, analyzed the "born classified" concept in a report to the Joint Committee and recommended that it be limited to nuclear weapons:

> The existence of a dual system of information control, one for "atomic" information and one for "defensive" information, has less validity now that other countries have developed capabilities of their own in military and peaceful uses of atomic energy. We would think it appropriate for both the Congress and the executive branch to explore the possibility of reinstituting a single information control system with uniformly applicable penal provisions for violations. The concept that information is "born" classified is not compatible with the expeditious action required to make information available for the full development of peaceful uses. This concept should be limited to nuclear weapons
>
> Therefore we recommend:
>
> 1. that the Commission remove all reactor technology from the restricted data category, including such areas as fuel element fabricating and processing techniques, leaving specific military applications of such technology to be protected, insofar as national security is involved, by the defense classification system;
>
> 2. that the Joint Committee reexamine the concept that atomic information in all fields is "born" classified; we believe that this concept is not compatible with the expeditious action required to permit rapid development of peaceful uses of atomic energy; and that therefore this

[12] Id. at 475.

concept should be limited to the design, manufacture, or utilization of atomic weapons; and

3. that the Joint Committee require the Commission to undertake the compilation of both classified and unclassified information relating to peaceful uses of atomic energy on a continuing and current basis so that it can be available in ready reference form for those entitled to use it.[13]

Following the panel's report, the Joint Committee held a series of hearings on the development, growth, and state of the atomic energy industry, using the occasion to elicit comments on the report of the McKinney panel. Responding to the panel's second recommendation K. E. Fields, General Manager of the AEC, set forth the views of the Commission on its meaning and implications:

> The concept of the panel as to what information is "born" classified needs some clarification. Its recommendation can be read to say the members of the panel thought all atomic energy information is considered classified until the particular report or document is declassified. We believe this was not meant, for the panel members know that much atomic information is considered unclassified from its beginning. Clearly, where the Commission has removed specific areas of information from the restricted data category, pursuant to section 142 of the act, information subsequently developed in those areas is not "born" classified.
>
> We assume, therefore, that this in effect is a recommendation that all atomic energy information, except in the weapons area, betreated as "born" unclassified. We also assume, because of the panel's first recommendation regarding control of information, that some atomic energy information of possible value in peacetime uses, for example, special military applications of reactor technology, should be classified under the defense classification system.
>
> This approach departs from the basic philosophy underlying the restricted data concept as expressed in both the 1946 and the 1954 acts. It takes from a civilian agency—the Commission—the practically exclusive power, outside the weapons utilization area, to determine what atomic energy information should be protected as sensitive information and what should be declassified and freely disseminated. Thus, under the present defense classification system prescribed by Executive Order 10501, then Defense Establishment would have discretion to determine whether reactor technology developed by it had military applications, and to keep classifications on it.
>
> The Commission does not believe that the classification principles prescribed by the 1954 act have interfered with the discharge of its statutory responsibility to encourage widespread participation in the development and utilization of

[13] U.S. Congress. Joint Committee on Atomic Energy. Peaceful Uses of Atomic Energy. Report of the Panel on the Impact of the Peaceful Uses of Atomic Energy Joint Committee Print, 84th Cong., 2d Sess. Washington, U.S. Govt. Print. Off., 1956. Vol. 1, p. 109.

atomic energy for peaceful purposes to the maximum extent consistent with the common defense and security.[14]

During hearings the following year, the Joint Committee heard two indictments of the "born classified" concept. In his prepared statement, V. Lawrence Parsegian, Chairman of Engineering Faculties and Professor of Nuclear Engineering at Rensselaer Polytechnic Institute, testified about the information "handicap" resulting from the "born classified" concept:

> The handicap I refer to does not arise from lack of enough declassified reports. Rather, it arises as a result of the restrictions that are inherent to the concept that reactor technology is 'born classified.' This means, in effect, that only the relatively few are permitted to know the status and problems of current reactor technology, and only these favored few are expected to have new ideas on developing these systems.
>
> The concept that reactor technology is 'born classified' is the same one which the McKinney panel—the panel on the impact of peaceful uses of atomic energy—deplored in its recent report to Congress.
>
> In my opinion, these limitations strike at the very roots of the elements that make for progress after the American pattern and should be eliminated as quickly as possible.
>
> I believe that this concept should be altered by revisions to the Atomic Energy Act of 1954. Revisions are needed to make the act a more positive and enabling instrument for current needs, because events have moved so fast since 1954.[15]

Parsegian also called attention to problems the "born classified" concept created in the areas of patents and inventions:

> Another serious weakness that results from information being 'born classified' has to do with invention, patent rights, and exploitation of patents.
>
> To begin with, relatively few patentable ideas seem to have been generated with classified reactor technology, despite the fact that this presents a 'happy hunting ground' for new ideas. It is my opinion that this is partly a result of secrecy restrictions, and partly because the act has excepted atomic inventions from normal patent practice.
>
> Even the ideas that are developed cannot be easily patented so long as they are classified. Worst of all, our Government and our citizens are losing out because they cannot make disclosures whereby to obtain foreign patent rights. Our patent position abroad is seriously weakening industry's competitive position.
>
> It is hoped that when reactor technology is declared unclassified, the patent sections of the act will also be changed to bring the atom within normal patent law and thereby to give

[14] Development, Growth, and State of the Atomic Energy Industry. Hearings Before the Joint Committee on Atomic Energy, 84th Cong., 2d sess. 380–381 (Feb. 29, March 1, 5, and 6, 1956). Part 2. Sec. 202 of the Atomic Energy Act of 1954 required the joint committee to conduct yearly hearings for the purpose of receiving information concerning the development, growth and state of the atomic energy industry.

[15] U.S. Congress. Joint Committee on Atomic Energy. Development, Growth, and State of the Atomic Energy Industry. Hearings, 85th Cong., 1st Sess., Part 1, Feb. 19, 20, 21, and 25, 1957. Washington, U.S. Govt. Print. Off., 1957. p. 175.

industry the inducements and help that are needed in this international race.

In conclusion, I would like to urge that Congress consider another revision of the Atomic Energy Act, one that will clearly define and limit the authority and role of Government, in order to reduce controls to the necessary minimum. In particular, there is need to eliminate the concept that information in to the reactor field is 'born classified' in order to bring the atomic effort the full support of our colleges and of our industries.[16]

Theodore S. Kenyon, a practicing patent lawyer, urged the removal of all secrecy restrictions on atomic energy information except those pertaining strictly to atomic weapons. He argued that secrecy retarded the flow of knowledge and advancement of atomic technology:

In 1953 when the 1954 act was being considered the House bill contained a clause with respect to the declassification of restricted data within 3 years, section 145c which read:

'No restricted data shall be so classified for more than three years after its origination or after its redesignation unless there is a specific finding made within six months preceding the end of any such three-year period that the common defense and security require that that restricted data retain its classification for an additional period of up to three years beyond the end of the preceding period.'

That provision was not enacted. Instead the declassification of restricted data was left to the Commission with the admonition, in sections 142a and b, to determine from time to time the data which can be published without undue risk and thereupon to cause such data to be declassified.

The Commission has established a declassification division which has worked valiantly to carry out this requirement. At first the division released data by the spoonful; more recently it has released data by the shovelful. But under the definition of restricted data contained in section 11 (r) every original thought concerning 'the use of special nuclear material in the production of energy' is 'born classified' and may not be uttered publicly until it has been passed through the mill of the declassification division.

The effect of this enforced secrecy on the teaching and dissemination and growth of knowledge of this science has been profound. Colleges and research centers have worked under serious handicap. Teaching and discussion have been limited to basic knowledge and material known to have been declassified. Education of advanced students faces the barrier of restriction on advance information. Scientists and engineers cannot communicate with one another except under the rigid controls of the Commission. As a practical matter, no one outside the officials of the declassification division knows with certainty what is declassified and what is not. Outsiders dare not publish an original thought or indeed anything except

[16] Ibid., p. 177–78.

> what they know to be stale. The tragedy is that in atomic science, where we need it as never before, and we are counting on the proven strength of our technology to lead the world, we are, by our own self-imposed law, strangling the very forces that are essential to our national purposes.[17]

The last Joint Committee hearings during which the concept of "born classified" was addressed specifically apparently occurred in 1958, when Professor V. L. Parsegian again appeared and urged less restriction on information:

> In summary:
>
> 1. Every effort should be made to enable universities, their faculties, and graduate students, to participate intimately in the wide range of basic research activities that contribute to the development of atomic energy, controlled thermonuclear fusion, rocket, and satellite programs. This is necessary both because the projects need this support and because graduate students must be better prepared to contribute to the newest technologies.
>
> 2. This requires that the vast systems of information controls be eliminated as a way of life, that secrecy be limited to weapons design and test, that basic research results be once more 'bornfree.' [18]

As long as most access to Restricted Data by private companies was limited to power reactor technology, it was not likely, from the Atomic Energy Commission standpoint, that the troublesome issue of privately generated information would arise. The national security implications of power reactor technology were limited essentially to protecting American interests in international competition for the power reactor market.

However, a more dangerous possibility arose in 1960 when several American companies began exploring the idea of research and development in the gas centrifuge process for producing uranium 235, a prime material for nuclear weapons. If the process could make it available at low cost in small, easily concealed plants, the U.S. objective of preventing nuclear weapon proliferation might be compromised.

The AEC staff proposed establishing a new category of classified information within the access program. In exchange for an access permit, each company would agree to make available to the Commission all technical data produced and grant the Government a nonexclusive, royalty-bearing license for its use of any invention or discovery. The staff noted, however, that "should a private firm not want access to AEC's Restricted Data in building a centrifuge, the limitations as to participation and AEC rights to information through controls or access permits would not apply."

In June 1960, the Commission agreed in principle that gas centrifuge technology would be incorporated in its access permit regulations (10 CFR Part 25), but with second thoughts about limiting application to companies seeking access to the AEC's Restricted Data.

---

[17] Ibid., p. 226–27.

[18] U.S. Congress. Joint Committee on Atomic Energy. Development, Growth, and State of the Atomic Energy Industry. Hearings, 85th Cong., 2d Sess., Feb. 19, 20, 21, 26, 28; Mar. 3 and 4, 1958. Washington, U.S. Govt. Print. Off., 1958. p. 142.

In November, the staff proposed that the amended Part 25 apply "to all permits for access to classified centrifuge information, whether or not the permittee desires access to AEC 'Restricted Data' information." Staff admitted that under existing regulations the Commission did "not require or take privately owned proprietary information or receive reports concerning the private activity," but contended the AEC's need for access to private information on the centrifuge made this exception necessary.

Neither Commission nor staff acknowledged the presence of the "born classified" concept, but it underlay their deliberations. In the Part 25 amendments, the Commission was implying, rather than announcing, that private research on the centrifuge would inevitably result in the generation of Restricted Data, which in turn would subject the private company to the terms of the regulation.

The proposed regulation, issued for public comment on December 13, 1960, did not make the point clear. When a number of commenting companies questioned the need for classification and the propriety of requiring AEC rights to technical data, the Commission decided to introduce one cautious statement of clarification. The terms and conditions for access would apply, it said, "irrespective of whether access to the Commission's Restricted Data information is desired." With this amendment the revised Part 25 became effective April 20, 1961.

By autumn 1963, the AEC's classification staff was growing uneasy about the effectiveness of the regulation. A few companies had contracts abroad to develop and manufacture nuclear devices that seemed to fall outside the Restricted Data domain of access; others were developing devices for purposes clearly unrelated to nuclear technology but which would be useful in producing fissionable materials and nuclear weapons. It felt that the easiest solution, declassification of these nonnuclear commercial application, would endanger national security by encouraging the proliferation of nuclear weapons. Staff also noted that many of the scientists and engineers involved had worked on classified AEC projects, and it thought declassification might encourage others to take their ideas to private industry, accelerating the spread of classified technology.

The alternative was "to make clear to the public that privately generated information *can* (sic) be Restricted Data and that dissemination by its originator is prohibited except as authorized by law." Staff suggested that Part 25 might be further amended to make it applicable only to Government-owned Restricted Data, and that a new regulation (Part 26) be drafted to cover Restricted Data generated by private companies or in foreign countries. Dissemination of privately generated Restricted Data would require a Commission permit, which it would grant if the action would not imperil the common defense and security.

This proposal reopened the question of the Commission's statutory authority in this area. In its preliminary justification, the staff relied entirely on the definition of Restricted Data in the 1954 act, and argued there was nothing in the legislative history of the 1946 act or the 1954 act to suggest that private work was meant to be outside it. Although the Attorney General had favored a clarifying amendment in 1947, he had decided that the Justice Department would proceed

on the interpretation that the term was applicable to private information.

In July 1964, the staff draft presented to the commissioners made clear for the first time the agency's interpretation of its statutory authority:

> The statutory definition is not limited to information within the scope of the definition that is generated or owned by the Commission or the Government. It includes also any information within the scope of the definition that is generated by any person even though he may never have been engaged in any Government atomic energy activity.

In the draft regulation, "Non-Part 25 Restricted Data" was defined as that act falling within the categories of Part 25: "(a) generated in privately sponsored work; (b) generated under Government contracts which permit such dissemination subject to security requirements; (c) owned by a Government contractor; and (d) of foreign origin."

The proposed Part 26 did not discuss its potential impact on the proprietary rights of individuals. Rather than publish the proposed regulation in the Federal Register for public comment, the Commission chose first to submit it privately to the Atomic Industrial Forum, which represented the major electric utilities and equipment manufacturers in the nuclear industry. Forum officials raised practical rather than constitutional issues, and the revised Part 26 which staff presented to the Commission in December 1964 met the Forum's criticisms point for point.

Commission approval of the new version of Part 26 on March 26, 1965, was on the condition that staff would discuss the question of legal authority with the Department of Justice. On June 4, Wayne Barrett in the Office of Legal Counsel at Justice told Franklin N. Parks, the Commission's legal expert on Part 25, that the department was "not completely satisfied that the Atomic Energy Act (1) was applicable to Private Restricted Data and (2) authorized the issuance of the proposed regulation."

Barrett set down his views systematically in a draft letter to the Commission, which he sent to Parks on September 30. In his informal response to the Commission's General Counsel, Parks admitted there was "substantial merit" in the arguments in Barrett's draft letter. He also thought Barrett had ignored the historical context in which the 1946 act had been drafted.

Early in 1966, Parks completed a memorandum which discussed in detail the Commission's authority to control dissemination of privately developed Restricted Data. It quoted extensively from the Senate hearings on the McMahon bill in 1946 and before the Joint Committee on revision of the act in 1954. The Commission sent the draft memorandum to the Justice Department in March 1966 and, after a series of meetings, department officials concluded the proposed regulations would be adequate if revised to delete specific references to criminal sanctions in the event the regulations were violated. In March 1967, the staff presented the AEC with a revised version of the 1965 proposal to amend Part 25 and issue the new Part 26.

Publication of the proposed regulation brought comment on statutory authority and constitutional issues. The atomic energy committee of the New York City Bar Association acknowledged the "born classified" feature of the statute to be unique, but observed the statute was silent on whether "born secret" data included that generated by individuals with no access to Government information and with no Government affiliation. All reports, testimony and hearings on the 1946 and 1954 acts were silent on this point. "The possible control of private data," it wrote, "was not a clearly identified issue before the Congress in 1946 and 1954 because the question of possible military significance of private data did not arise until important private research and development efforts were commenced—after the passage of the 1954 act."

Attempting to meet these and other objections, Parks and other Commission attorneys drafted revisions during the summer and fall of 1967. Members of the staff criticized sharper definitions they said would leave loopholes through which Restricted Data might escape to the public. One proposal that received considerable attention was to use no-fund contracts to control the dissemination of Private Restricted Data. No-fund contracts, it was argued, could be tailor-made for each case, would provide better controls, and had been used effectively before the access permit system was established.

However, further study in the General Counsel's office disclosed flaws in all these claims. Legal staff could cite several sections of the proposed regulations that offered more flexibility than the contract approach. Terms of a contract could be varied to fit individual circumstances, but the basis for variation would have to be objectively justified if the contract method was to avoid constitutional objections. Further, the General Counsel maintained that a regulation requiring private individuals to enter into a contract would be "very unorthodox."

A revised regulation was published in December 1967, but public comment revealed that the staff's attempts to satisfy earlier reservations about statutory authority and constitutionality had not succeeded. Yet another revision of the proposed Part 26 was reviewed by the commissioners in January 1969 but left them unconvinced. Once again, the statutory and constitutional questions were referred to outside legal authorities for study.

It was the last deferral. Larger and equally perplexing questions had now arisen about how to transfer the Government's huge uranium enrichment facilities to private industry and how to control isotope separation technology in general. Late in the year, an entirely new problem arose when KMS Industries, Inc., a Michigan research group, consulted the AEC about work it was doing on controlled thermonuclear reactions. Because this research using high-power, short-pulsed lasers had potential applications in the design of thermonuclear weapons, the Commission once again found a private company producing information that was "born classified."

Part 26, which might have helped in the KMS case and others involving lasers, was never promulgated. Instead, the AEC reverted to its 1950's practice of negotiating no-fund contracts to provide a legal basis for controlling the dissemination of Restricted Data. No further significant changes in the AEC's classified information policy were attempted before the agency was abolished in 1975.

D. THE PROGRESSIVE MAGAZINE CASE

1. Preface

Many countries began to acquire nuclear power plant technology in the decade following passage of the Atomic Energy Act of 1954. "At the same time," writes William Sweet in Editorial Research Reports, "nuclear weapons—including U.S. tactical weapons—were becoming more widely dispersed throughout the world." He continues:

> Britain, then France, and finally China tested their first atomic bombs, and then their first hydrogen bombs. With technology and information more widely disseminated, people began to warn that soon we would be living in a "world of nuclear powers." Such fears, and—at a more concrete level—anxiety that West Germany would be the next country to "go nuclear," contributed first to discussion and then negotiation of a treaty to prevent the spread of atomic weapons. The Non-Proliferation Treaty (NPT) was concluded in 1968.[19]

The NPT in effect conceded that atomic knowhow was already, for all practical purposes, in the public domain. In attempted to control not atomic information, but the materials needed to produce atomic bombs. The NPT called for a safeguards system of monitoring and inspection "with a view to preventing diversion of nuclear energy from peaceful uses to nuclear weapons or other nuclear explosive devices." It said nothing about hydrogen bombs as a special item.

Until the Progressive case broke, hydrogen bombs apparently were given no special attention as a proliferation problem.

> Hydrogen bombs, in fact, have received remarkably little discussion in the literature on nuclear proliferation. Among six major studies of the nuclear proliferation problem which have appeared since 1974, none contains a chapter or paper devoted to the subject of thermonuclear explosives. Theodore B. Taylor, who more than any other individual has explored the types of equipment, technology, and expertise needed to build atomic bombs, makes no mention at all of hydrogen bombs as they are designed today in the book on nuclear safeguards that he wrote with Mason Willrich in 1974. The book contains a half-page discussion of "pure fusion" bombs—a type of hydrogen bomb, as yet undeveloped, which would require no fission-bomb trigger. But it concludes that this type of explosive probably could not be made any time in the foreseeable future "without highly sophisticated equipment and exceptionally highly skilled and experienced specialists." [20]

Sweet surmises that disinterest in hydrogen bombs on the part of students of proliferation "may reflect the view that once a country has acquired atomic bombs, the prerequisite for construction of a hydrogen bomb, the damage already is done." It also may reflect a view

> that the hydrogen bomb secret is a rapidly vanishing commodity, and that any attempt to prevent construction of

[19] Sweet. Op. Cit., p. 655.

[20] Sweet. *Op. Cit.*, p. 656. Sweet states that an Office of Technology Assessment study of nuclear proliferation which appeared in 1977 makes no mention of H-bombs. Of the remaining four studies, three mention H-bombs only in passing, and the fourth devotes just four pages to them.

> hydrogen bombs once a country already has produced an atomic bomb is bound to fail. Since 1945, the time it has taken a country to test an H-bomb once it has tested an A-bomb has tended to decline, although France is an exception.[21]

Whatever the explanation, it was not the position the Government took in the Progressive case.

The Department of Energy later explained it believes there is a powerful link between the "born classified" concept and prevention of nuclear proliferation. It declared in a June 1980 letter to the subcommittee chairman:

> The Department firmly believes that the concept is as vital to the protection of the national security today, in an era of nuclear proliferation and terrorism, as it was during the post-World War II period of its conception. The grave danger to the nation posed by the proliferation of nuclear weapons information has been more keenly recognized in the last few years than ever before. The Treaty on the Nonproliferation of Nuclear Weapons and the Nonproliferation Act of 1978 evidence clear Congressional and Executive Branch concern over the ever-spreading capability of national and subnational groups to produce or acquire nuclear weapons. Most recently, of course, the Executive Branch has demonstrated its strong policy against proliferation by its attempts to enjoin publication of weapon design information generated by private citizens in the *United States of America* v. *The Progressive, Inc., et al*, and *United States of America* v. *Independent Berkeley Student Publishing Co., Inc.* Although the Government's efforts were thwarted by publication of sensitive material by a third party which mooted the law suits, the Government was successful in achieving court enforcement of the Atomic Energy Act provisions regarding Restricted Data in both cases.[22]

2. Chronology [23]

In February 1979, Howard Morland, a free-lance writer specializing in energy and nuclear weapons matters, finished an article describing how a hydrogen bomb works. The article, entitled "The H-Bomb Secret—How We Got It, Why We're Telling It," written while Morland was on assignment for The Progressive magazine, was the product of independent research.

On February 27, a copy of it was delivered to the Department of Energy (DOE) for verification of the technical accuracy of its account of hydrogen weapon design and manufacture. DOE reviewers determined that portions of the article contained Restricted Data. On March 1, DOE General Counsel telephoned editors of The Progressive and informed them that, in the view of DOE, the Department of State

---

[21] Id., p. 657.

[23] This section draws upon *The Progressive Case: Legal Issues*, an analysis prepared by Kent M. Ronhovde, legislative attorney in the American Law Division, Congressional Research Service, Library of Congress, at the request of the Subcommittee on Government Information and Individual Rights of the House Committee on Government Operations (Feb. 14, 1980)..

[22] Letter to Chairman Preyer from Richard G. Hewlett, DOE Chief Historian (retired), submitting the Hewlett born-classified study. See Hearings.

and the Arms Control and Disarmament Agency, publication of the Restricted Data portions of the article would injure the United States and give advantage to other nations. To conform to U.S. policy of striving to prevent the proliferation of nuclear weapons, the magazine was asked to refrain from publishing the article.

In a subsequent meeting, DOE representatives informed the publisher and editors of The Progressive that publication would constitute a violation of the Atomic Energy Act and give advantage to foreign countries in the development of thermonuclear technology. They were advised that excission and recasting of portions of the article would eliminate the need for classification and allow publication to go forward. The magazine later informed DOE that it intended to publish the Morland article in its entirety.

On March 9, the Justice Department obtained a temporary restraining order in the U.S. District Court for the Western District of Wisconsin against the Madison-based magazine. An *in camera* hearing was held March 23, and three days later U.S. District Judge Robert Warren issued a preliminary injunction.[24] The Progressive appealed to the Seventh Circuit Court of Appeals, and sought but was denied an expedited hearing. The magazine then petitioned the Supreme Court for a writ ordering an expedited appeal, claiming that parties who have been enjoined from engaging in constitutionally protected speech have a right to prompt appellate review of that injunction. This motion was denied when the Supreme Court held in a *per curiam* opinion (with two justices dissenting) that because of petitioner delays in the filing of motions and submission of briefs they "forbore any right to expedition that the Constitution might otherwise have afforded them." *Morland* v. *Sprecher*, 47 U.S.L.W. 3838 (No. 78–1904, filed July 2, 1979).

The Seventh Circuit Court of Appeals heard oral argument in the case on September 13, but the appellate process was being overtaken by events. On August 27, a California computer programmer named Charles Hansen sent a letter on thermonuclear weapon design to three Members of Congress and to several newspapers which disclosed substantially the same Restricted Data that was contained in the Morland article. The DOE attempted to notify each recipient of the letter that its contents were classified and that publication would cause harm. When its publication by a student-oriented Berkeley newspaper, The Daily Californian, appeared imminent, the Justice Department sought and on September 15 obtained a temporary restraining order from Judge Robert H. Schnacke of the U.S. District Court for the Northern District of California prohibiting publication of the letter. However, on learning of this order The Madison Press Connection, a Wisconsin paper, which was not one of the known recipients of the Hansen letter, published it the next day.

On September 17, the Justice Department announced it would stop trying to restrain publication of the H-bomb technology at issue. Accordingly, the Government sought dismissal of the preliminary injunction against publication of the Morland article and the temporary restraining order against publication of the Hansen letter. It concluded that the case against The Progressive had been rendered

[24] *United States* v. *Progressive, Inc.*, 467 F. Supp. 990 (W.D. Wis. 1979).

moot by publication of the basic secrets underlying the dispute. At the same time, the Justice Department announced it would undertake a criminal inquiry into possible violations of the Atomic Energy Act and of the court orders in the two cases.

Meanwhile, The Progressive has pursued efforts to have sealed portions of the record in its case opened to the public and, as of August 1980, the matter is unresolved. Thus, while the suit against the magazine has been concluded, the issues it raised remain controversial. As Newsweek summarized it, "[t]his was in the classic legal maxim, a hard case that can make bad law. But so many questions are left unresolved by its aborted conclusion that even harder tests could yet follow." (Oct. 1, 1979, at 45).

3. The First Amendment [25]

In his opinion Judge Warren stated: "Under the facts here alleged, the question before this court involves a clash between allegedly vital security interests of the United States and the competing constitutional doctrine against prior restraint in publication." The clash between national security interests and First Amendment freedoms presented in Progressive is not new to the courts, but it has been litigated rarely, and with less than clear results.

The First Amendment to the Constitution provides that "Congress shall make no law . . . abridging the freedom of speech, or of the press . . ." The language of the Amendment is sparse and has generated a great deal of judicial controversy as to the extent of its intended application. Of the original intention of the drafters it has been said that "[i]nsofar as there is likely to have been a consensus, it was no doubt the common law view as expressed by Blackstone." (The Constitution of the United States of America, Analysis and Interpretation, S. Doc. 92–82, 92d Cong., 2d Sess. 936 (1973)). Blackstone's Commentaries on the Laws of England includes the statement that "the liberty of the press is indeed essential to the nature of a free state; but this consists in laying no previous restraints upon publications, and not in freedom from censure for criminal matter when published." He added: "To subject the press to the restrictive power of a licenser, as was formerly done, both before and since the revolution, is to subject all freedom of sentiment to the prejudices of one man, and make him the arbitrary and infallible judge of all controverted points in learning, religion and government. But to punish . . . any dangerous or offensive writings, which, when published, shall on a fair and impartial trial be adjudged of a pernicious tendency, is necessary for the preservation of peace and good order, of government and religion, the only solid foundations of liberty." (4 Blackstone, Commentaries on the Laws of England, at 138–139 (London: 1813)). Today, while prior restraints are subjected to greater scrutiny, the modern position of the Supreme Court recognizes the view that "the Amendment operates not only to bar most prior restraints of expression but subsequent punishment of all but a narrow range of expression" as well. (S. Doc. 92–82, supra, at 938).

Early opinions of the Supreme Court reflected the Blackstone outlook. Thus Justice Holmes, in *Patterson* v. *Colorado*, 205 U.S. 454 (1907), wrote that the main purpose of provisions such as the First

[25] This analysis follows Ron hovde, op. cit.

Amendment protection of speech "is to prevent all such previous restraints upon publications as had been practiced by other governments . . ." (at 462). Twelve years later, in *Schenck* v. *United States*, 249 U.S. 47 (1919), Holmes said: "it may well be that the prohibition of laws abridging the freedom of speech is not confined to previous restraints, although to prevent them may have been the main purpose, . . ." (at 51–52). The often quoted language of the Justice then followed: "[T]he character of every act depends upon the circumstances in which it is done. *Aikens* v. *Wisconsin*, 195 U.S. 194, 205, 206. The most stringent protection of free speech would not protect a man in falsely shouting fire in a theatre causing panic. It does not even protect a man from an injunction against uttering words that may have all the effect of force. *Gompers* v. *Bucks Stove & Range Co.*, 221 U.S. 418, 439. The question in every case is whether the words used are used in such circumstances and are of such a nature as to create a clear and present danger that they will bring about the substantive evils that Congress has a right to prevent. It is a question of proximity and degree." [26] (at 52). Thus, as the Court summarized in *Chaplinsky* v. *New Hampshire*, 315 U.S. 568, 571 (1942), "the right of free speech is not absolute at all times and under all circumstances."

But the Court has made it clear that any "system of prior restraints comes to this Court bearing a heavy presumption against its constitutional validity." *Bantam Books, Inc.* v. *Sullivan*, 372 U.S. 58, 70 (1968). And in *Nebraska Press Association* v. *Stuart*, 427 U.S. 539 (1976), the Court recently added that "the damage can be particularly great when the prior restraint falls upon the communication of news and commentary on current events." (at 559) At issue in *Progressive* was essentially the question whether the Government could overcome the strong presumption running against its prior restraint. For while the so-called "doctrine of prior restraint" suggests that procedures used to suppress speech must rely on subsequent sanctions rather than prepublication restriction, the doctrine has been recognized to include an ill-defined exception for extraordinary situations.

The leading case in which the Supreme Court has wrestled with the nature of this exception is *Near* v. *Minnesota*, 283 U.S. 697 (1931). In dealing with an appeal of an injunction barring publication of a newspaper as a result of its allegedly defamatory articles, the Court suggested areas in which prior restraint on speech could be condoned. Chief Justice Hughes wrote: "No one would question but that a government might [in time of war] prevent actual obstruction to its recruiting service or the publication of the sailing dates of transports or the number and location of troops. On similar grounds, the primary requirements of decancy may be enforced against obscene publications. The security of the community life may be protected against incitements to acts of violence and the overthrow by force of orderly government." (at 716).

While this language is frequently cited as an indication that national security may in certain circumstances justify imposition of prior restraints, it should be pointed out that the Court in *Near* went on to strike down the injunction as violative of the First Amendment, and in doing so said: "The question is whether a statute authorizing such proceedings in restraint of publication is consistent with the conception

[26] *Schenck* dealt with crimes alleged to have been committed during time of war.

of liberty of the press as historically conceived and guaranteed. In determining the extent of the constitutional protection, it has been generally, if not universally, considered that it is the chief purpose of the guarantee to prevent previous restraints upon publication." (at 713). And the Court added that "[t]he fact that the liberty of the press may be abused by miscreant purveyors of scandal does not make any the less necessary the immunity of the press from previous restraint in dealing with official misconduct. Subsequent punishment for such abuses as may exist is the appropriate remedy, consistent with constitutional privilege. (at 720).

In *Gitlow* v. *New York*, 268 U.S. 652 (1925), it was said that "a State may punish utterances endangering the foundations of organized government and threatening its overthrow by unlawful means. These imperil its own existence as a constitutional State. Freedom of speech and press . . . does not protect publications or teachings which tend to subvert or imperil the government or to impede or hinder it in the performance of its governmental duties." (at 667). And Justice Brandeis, concurring in *Whitney* v. *California*, 274 U.S. 357 (1927) (overruled, *Brandenburg* v. *Ohio*, 395 U.S. 444 (1969)), suggested that free speech rights were subject to restriction "if the particular restriction proposed is required in order to protect the State from destruction or from serious injury, political, economic, or moral." (at 373).

In *New York Times Co.* v. *United States*, 403 U.S. 713 (1971), the Supreme Court's per curiam opinion refused to subordinate the First Amendment interest to an asserted national security interest in suppression of publication of the so-called "Pentagon Papers." Six concurring opinions were filed, Justices Harlan, Blackmun, and Chief Justice Burger filing dissents. The per curiam opinion reads:

> We granted certiorari in these cases in which the United States seeks to enjoin the New York Times and the Washington Post from publishing the contents of a classified study entitled "History of U.S. Decision-Making Process on Viet Nam Policy."
>
> Any system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity, *Bantam Books, Inc.* v. *Sullivan*, 372 U.S. 58, 70 (1963); see also *Near* v. *Minnesota*, 283 U.S. 697 (1931). The Government "thus carries a heavy burden of showing justification for the imposition of such a restraint." *Organization for a Better Austin* v. *Keefe*, 402 U.S. 415, 419 (1971). The District Court for the Southern District of New York in the *New York Times* case and the District Court for the District of Columbia Circuit in the *Washington Post* case held that the Government had not met that burden. We agree.

The Government argued at the district court level that enjoining publication was authorized by a provision of the Espionage Act of 1917 (40 Stat. 217), namely 18 U.S.C. 793(e), and alternatively that the Government could utilize the inherent power in the Executive to protect the national security. The use of section 793 was found inappropriate by the lower court (both for its language and its legislative history) and the latter contention was also found inapplicable to the case at bar, the court citing the language of *Grosjean* v. *American Press Co., Inc.*, 297 U.S. 233 (1936):

> The predominant purpose of the . . . (First Amendment) was to preserve an untrammeled press as a vital source of public information. The newspapers, magazines, and other journals of the country, it is safe to say, have shed and continue to shed, more light on the public and business affairs of the nation than any other instrumentality of publicity; and since informed public opinion is the most potent of all restraints upon misgovernment, the suppression or abridgement of the publicity afforded by a free press cannot be regarded otherwise than with grave concern. (at 250).

In the final analysis the lower court simply found insufficient national security interest at stake: "Fortunately upon the facts adduced in this case there is no sharp clash such as might have appeared between the vital security interest of the Nation and the compelling constitutional doctrine against prior restraint." *United States* v. *New York Times Company*, 328 F. Supp. 324 (S.D.N.Y. 1971).

While the per curiam opinion in *New York Times* sheds little light on the Court's thinking as to the breadth of the exception to the prior restraint doctrine, some of the concurring and dissenting opinions contain language which may be instructive.

Justice Black argued that the word "security" constitutes but a "vague generality whose contours should not be invoked to abrogate the fundamental law embodied in the First Amendment." He concluded that the "guarding of military and diplomatic selects at the expense of informed representative government provides no real security for our Republic. The Framers of the First Amendment, fully aware of both the need to defend a nation and the abuses of the English and Colonial governments, sought to give this new society strength and security by providing that freedom of speech, press, religion, and assembly should not be abridged." (Concurring opinion of Justice Black, at 719). Justice Douglas, expressing similar sentiments regarding the principles of the Amendment, suggested that the documents themselves may not have been of a nature to warrant exceptional treatment:

> There are numerous sets of this material in existence and they apparently are not under any controlled custody. Moreover, the President has sent a set to the Congress. We start then with a case where there already is rather wide distribution of the material that is destined for publicity, not secrecy. I have gone over the material listed in the in camera brief of the United States. It is all history, not future events. None of it is more recent than 1968. (Concurring opinion of Justice Douglas, at 722, n. 3).

And Justice Brennan also saw the First Amendment as an "absolute bar" in this particular type of case: "The entire thrust of the Government's claim throughout these cases has been that publication of the material sought to be enjoined 'could,' or 'might,' or 'may' prejudice the national interest in various ways. But the First Amendment tolerates absolutely no prior judicial restraints of the press predicated upon surmise or conjecture that untoward consequences may result." (at 725–726). But in rejecting the circumstances prevailing in that case, Brennan did address the threat of atomic war

indirectly "Even if the present world situation were assumed to be tantamount to a time of war, or if the power of presently available armaments would justify even in peacetime the suppression of information that would set in motion a nuclear holocaust, in neither of these actions has the Government presented or even alleged that publication of items from or based upon the materials at issue would cause the happening of an event of that nature." (at 726). Even in such a situation, said Brennan, "only governmental allegation and proof that publication must inevitably, directly, and immediately" cause the occurrence of the event would support injunctive relief. (Id.) The standard of "direct, immediate, and irreparable damage to our Nation or its people" was echoed by Justice Stewart in his concurrence. (at 730).

Justice White, concurring, placed emphasis on the absence of congressional authority for the restraint: "I do not say that in no circumstances would the First Amendment permit an injunction against publishing information about government plans or operations. Nor, after examining the materials the Government characterizes as the most sensitive and destructive, can I deny that revelation of these documents will do substantial damage to public interests. Indeed, I am confident that their disclosure will have that result. But I nevertheless agree that the United States has not satisfied the very heavy burden that it must meet to warrant an injunction against publication in these cases, at least in the absence of express and appropriately limited congressional authorization for prior restraints in circumstances such as these." (at 731) (As will be discussed, the attempts made to enjoin publication of The Progressive were in fact based upon portions of the Atomic Energy Act.) Justice Marshall in his concurrence dealt almost exclusively with the significance of an absence of legislation, and cited the refusal of the Congress on two occasions to enact a law that would have given the Executive the authority it sought in this case. (Concurring opinion of Justice Marshall, at 740–748).

In dissent, the Chief Justice and Justices Harlan and Blackmun were critical of the haste and pressures under which the case was concluded. But Justice Harlan also stressed the need to accord greater deference to the decisions of the Executive in matters of this kind:

> I agree that, in performance of its duty to protect the values of the First Amendment against political pressures, the judiciary must review the initial Executive determination to the point of satisfying itself that the subject matter of the dispute does lie within the proper compass of the President's foreign relations power. Constitutional considerations forbid 'a complete abandonment of judicial control.' *Cf. United States* v. *Reynolds*, 345 U.S. 1, 8 (1953). Moreover, the judiciary may properly insist that the determination that disclosure of the subject matter would irreparably impair the national security be made by the head of the Executive Department concerned . . . after actual personal consideration by that officer. This safeguard is required in the analogous area of executive claims of privilege for secrets of state . . . But in my judgment the judiciary may not properly go be-

yond these two inquiries and redetermine for itself the probable impact of disclosure on the national security. (at 757).

New York Times is pertinent to the issues posed by *Progressive* in that it elucidates what little case law exists to be relied on, demonstrates the diversity of opinion which exists even among those arriving at similar results, and suggests that such result in any given case will in large measure depend on delicate shadings of factual circumstances giving rise to the controversy.

Central to the magazine's contentions in *Progressive* was that publication of the article did not rise to the level of immediate, direct irreparable harm needed to justify treading on First Amendment rights. Judge Warren disagreed:

> Does the article provide a "do-it-yourself" guide for the hydrogen bomb? Probably not. A number of affidavits make quite clear that a sine qua non to thermonuclear capability is a large, sophisticated industrial capability coupled with a coterie of imaginative, resourceful scientists and technicians. One does not build a hydrogen bomb in the basement. However, the article could possibly provide sufficient information to allow a medium size nation to move faster in developing a hydrogen weapon. It could provide a ticket to by-pass blind alleys.
>
> The Moreland piece could accelerate the membership of a candidate nation in the thermonuclear club. Pursuit of blind alleys or failure to grasp seemingly basic concepts have been the cause of many inventive failures. *United States* v. *Progressive, Inc.*, supra, at 993–994.

The opinion also rejected the magazine's stated motives for publication:

> Defendants have stated that publication of the article will alert the people of this country to the false illusion of security created by the government's futile efforts at secrecy. They believe publication will provide the people with needed information to make informed decisions on an urgent issue of public concern.
>
> However, this Court can find no plausible reason why the public needs to know the technical details about hydrogen bomb construction to carry on an informed debate on this issue. Furthermore, the Court believes that the defendants' position in favor of nuclear nonproliferation would be harmed, not aided, by the publication of this article. (at 984).

Judge Warren differentiated the article from the material at issue in *New York Times* by suggesting that the latter was primarily historical and was more likely to "embarrass" the United States than to affect seriously its national security.

Early in his opinion Judge Warren quotes from Justice Frankfurter's dissent in *Bridges* v. *California*, 314 U.S. 252, 282 (1941): "Free speech is not so absolute or irrational a conception as to imply paralysis of the means for effective protection of all the freedoms secured by the Bill of Rights." The idea of a "hierarchy of values" within the Bill of Rights is central to his argument that life is more

important than free speech: "Faced with a stark choice between upholding the right to continued life and the right to freedom of the press, most jurists would have no difficulty in opting for the chance to continue to breathe and function as they work to achieve perfect freedom of expression. . . . The case at bar is so difficult precisely because the consequences of error involve human life itself and on such an awesome scale." (at 995). Warren's decision is ultimately couched in the terms of *Near* v. *Minnesota:*

> In the *Near* case, the Supreme Court recognized that publication of troop movements in time of war would threaten national security and could therefore be restrained. Times have changed significantly since 1931 when *Near* was decided. Now war by foot soldiers has been replaced in large part by war machines and bombs. No longer need there be any advance warning or any preparation time before a nuclear war could be commenced.
>
> In light of these factors, this Court concludes that publication of the technical information on the hydrogen bomb contained in the article is analogous to publication of troop movements or locations in time of war and falls within the extremely narrow exception to the rule against prior restraint. (at 996).

The court thus found the "direct, immediate and irreparable harm" described in *New York Times.*

In a recent decision the Supreme Court commented on the nature of the clear and present danger test as it is perceived today: "Mr. Holmes' test was never intended 'to express a technical legal doctrine or to convey a formula for adjudicating cases.' *Pennekamp* v. *Florida*, 328 U.S. 331, 353 (1946) (Frankfurter, J., concurring). Properly applied, the test requires a court to make its own inquiry into the imminence and magnitude of the danger said to flow from the particular utterance and then to balance the character of the evil, as well as its likelihood against the need for free and unfettered expression." *Landmark Communications, Inc.* v. *Virginia*, 435 U.S. 829, 842–843 (1978).

At the subcommittee hearings, press lawyer Floyd Abrams testified:

> The notion that the Government need not prove, in Justice Stewart's words, that the materials sought to be suppressed would surely result in direct and immediate and irreparable harm to the Nation and its people and that all it need claim is that the material by its nature is restricted and hence subject to restraint and criminal punishment is, in my view, constitutionally unacceptable.[27]

4. Secrecy Provisions of the Atomic Energy Act

The Government's suit to stop publication of The Progressive article was based on authority of the Atomic Energy Act.[28] That act provided

[27] Hearings.

[28] The Atomic Energy Act, so-called, is the product of the Atomic Energy Act of 1946 (60 Stat. 755) and the Atomic Energy Act of 1954 (68 Stat. 919), as variously amended over the years. It is codified at 42 U.S.C. 2011 et seq. Also, it should be noted that in 1974 the Atomic Energy Commission (referred to frequently in the United States Code provisions) was abolished (Act of Oct. 11, 1974, Public Law 93–438, Title I, Sec. 104(a), 88 Stat. 1237, 42 U.S.C. 5811 et seq.). Its functions and personnel were transferred to the Energy Research and Development Administration (ERDA) andn the Nuclear Regulatory Commission (NRC). ERDA has since become a part of the Department of Energy (42 U.S.C. 7151).

it was to be the policy of the Atomic Energy Commission (see footnote below) "to control the dissemination and declassification of Restricted Data in such a manner as to assure the common defense and security." (42 U.S.C. 2161). "Restricted Data" is defined as "all data concerning (1) design, manufacture, or utilization of atomic weapons; or (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy but shall not include data declassified or removed from the Restricted Data category..." (42 U.S.C. 2014(y)) (Emphasis added).

Authority for the injunctive remedy is provided by the Act as 42 U.S.C. 2280 which provides:

> Whenever in the judgment of the Commission any person has engaged or is about to engage in any acts or practices which constitute or will constitute a violation of any provision of this chapter, or any regulation or order issued thereunder, the Attorney General on behalf of the United States may make application to the appropriate court for an order enjoining such acts or practices, or for an order enforcing compliance with such provision, and upon a showing by the Commission that such person has engaged or is about to engage in any such acts or practices, a permanent or temporary injunction, restraining order, or other order may be granted.

The violation alleged to have been involved in publication of the article is set out at 42 U.S.C. 2274:

> Whoever, lawfully or unlawfully, having possession of, access to, control over, or being entrusted with any document, writing, sketch, photograph, plan, model, instrument, appliance, note, or information involving or incorporating Restricted Data—
>
> (a) communicates, transmits, or discloses the same to my individual or person, or attempts or conspires to do any of the foregoing, with intent to injure the United States or with intent to secure an advantage to any foreign nation, upon conviction thereof, shall be punished by imprisonment for life, or by imprisonment for any term of years or a fine of not more than $20,000 or both;
>
> (b) communicates, transmits, or discloses the same to any individual or person, or attempts or conspires to do any of the foregoing, with reason to believe such data will be utilized to injure the United States or to secure an advantage to any foreign nation, shall, upon conviction, be punished by a fine of not more than $10,000 or imprisonment for not more than ten years, or both.[29]

The Government contended in its suit that The Progressive was about to violate 42 U.S.C. 2274(b) and that since the statutory elements had been met the Government was entitled to an injunction under 42 U.S.C. 2280. Great emphasis was placed on the existence of these statutes as a distinguishing factor between *New York Times* and this suit:

[29] Other related provisions include (1) 42 U.S.C. 2275: Receipt of Restricted Data; (2) 42 U.S.C 2276: Tampering with Restricted Data; (3) 42 U.S.C. 2277; Disclosure of Restricted Data (public servants).

> In the circumstances at bar, the Executive is not acting solely pursuant to its inherent power to protect the national security. It invokes the aid of this court to protect against disclosure of Restricted Data which Congress has determined should not be disseminated and which Congress has given the courts the means to protect through entry of injunctive relief prohibiting such release. In enacting the Atomic Energy Act, Congress recognized the grave consequences which might result from the dissemination of sensitive information pertaining to the development of Atomic weaponry. Congress, therefore, not only made it a crime to disclose such information, but also authorized injunctive relief to ensure that the harm to the nation be prevented. This legislative finding, even where there is a resulting restriction on an individual's freedom of speech, is entitled to judicial deference. (*Plaintiffs Statement of Points and Authorities*, at 11).

Also stressed was the distinction between primarily "historical" information at issue in *New York Times* as opposed to the "technical information" involved in *Progressive*. (*Id.*, at 13).

The defendants sought to distinguish the statutes relied upon from the statutory authority required under some of the New York Times language:

> While Justice White concluded that the government had not met its burden of proof in *New York Times* "at least in the absence" of congressional authorization for prior restraint, he emphasized that the Court would not accept just any statutory justification for the imposition of such an extraordinary remedy. It had to be "express." It had to be "appropriately limited." 403 U.S. at 731. Statutory authorization for prior restraint, in other words, requires a clear, comprehensive, and constitutional expression of the will of Congress, constitutional in the light of the First Amendment. *See Id.* at 730 (Stewart, J., concurring). That expression of congressional will does not appear in the Atomic Energy Act of 1954.
>
> The Act prohibits the communication, transmission or disclosure of "Restricted Data." 42 U.S.C. 2274. It does not specifically prohibit publication. (Defendants' Memorandum Brief in Opposition to the Government's Application for a Preliminary Injunction, at 25–26).

Whether prior restraint of publication was envisioned by Congress is unclear, and case law is equally unavailing, the only previously reported case under section 2274 have involved espionage. See *Gessner* v. *United States*, 354 F.2d 726 (10th Cir. 1965).

In analyzing the espionage statutes, authors Edgar and Schmidt found nothing in voluminous legislative history of the Atomic Energy Act to shed light on the intended application of 42 U.S.C. 2274: "nothing in the legislative history bears on the question whether publication should be considered a communication 'to any . . . person . . . with reason to believe such data will be utilized to injure the United States etc.,' in violation of subsection 2274(b)." (Edgar and Schmidt,

"The Espionage Statutes and Publication of Defense Information," 73 *Columbia Law Review* 929, 1075 (1973).[30]

Judge Warren simply stated that "the Court finds that the statute in question is not vague or overbroad. The Court is convinced that the terms used in the statute—'communicates, transmits or discloses'—include publishing in a magazine." (467 F. Supp., at 994). "The Government has met its burden under section 2274 of the Atomic Energy Act." (at 996). Both sides to the controversy argued that the legislative history provided support for their position, but no language was cited which could be said to be clearly dispositive of congressional intent.

The absence of reported case law under either section 2274 or 2280 suggests a void in judicial interpretation as well, leaving analogy to the espionage laws as the only potentially fruitful research prospect. A study of arguments on those provisions, Ronhovde of the Congressional Research Service reports in his analysis, "reveals little consensus in interpretation and requires acceptance of construction by analogy in any event—a methodology of dubious merit in the assessment of congressional intent." [31]

5. The Public Domain v. Born Classified

In 1951, through the issuance of Executive Order 10290, President Truman extended the coverage of the classification system to nonmilitary agencies which had a role in "national security" matters. The directive cited no specific constitutional or statutory authority for its promulgation. Instead, the Chief Executive relied upon implied powers such as the "faithful execution of the laws" clause. (Indeed, the Trading with the Enemy Act, 40 Stat. 411, a World War I law that authorized the President to designate patents to be kept secret, appears to have been the first direct statutory grant of authority to the Executive to declare a type of information secret. Ironically, utilization of this authority was placed in civilian, not military hands.[32]

The current national security information manifest, President Carter's EO 12065, lays down a classification system whose stated purpose is to "balance the public's interest in access to Government information with the need to protect certain national security information from disclosure." The order acknowledges only one outside authority for classification: "Except as provided in the Atomic Energy Act of 1954, as amended, this Order provides the only basis for classifying information." (Section 1–101). The order designates classifica-

[30] These authors analyzed the issue as it arose in the context of 18 U.S.C. 793 (d) and (e), sections containing the same undefined use of "communication," in *New York Times*. They concluded not only that publication should be included within the meaning of the statute, but that to construe it otherwise would undermine the feasibility of having any such proscription. See 73 *Columbia Law Review*, at 1033–1036. For additional discussion, see "Criminal Code Reform Act of 1977," Report of the Senate Judiciary Committee, S. Rep. No. 95–605, 95th Cong., 1st Sess. at 215, n. 10.

[31] Ronhovde, op. cit.

[32] The act provided for the President to designate patents, the publication of which might "be detrimental to the public safety or defense, or may assist the enemy or endanger the successful prosecution of the war," to be kept secret. Harold C. Relyea of the Congressional Research Service writes: "No label was devised for this action. Quite the contrary, the means provided for maintaining this secrecy was to 'withhold the grant of a patent until the end of the war'. This would appear to be the first direct statutory grant of authority to the Executive to declare a type of information secret. Also, although the provision pertained to defense policy, utilization of this authority was placed in civilian, not military hands." Relyea, Government Information Security Classification Policy. In U.S. Congress. Senate. Supplementary Reports On Intelligence Activities Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities. Rep. No. 94–755, 94th Cong., 2d Sess. (April 23, 1976). Book VI, p. 323.

tion categories (i.e., "top secret," "secret," and "confidential") and limits original classification authority to described persons.

The Atomic Energy Act deals with the principle of information classification somewhat differently. Rather than describing types of information which "should" be classified at a certain level of secrecy, the act merely defines the subject matter which is in fact to be considered Restricted Data. That is, all data concerning X, Y and Z is by definition considered Restricted Data unless expressly declassified or removed from that category—hence, "born classified" by virtue of its subject matter alone, without regard to its source.[33] It was in light of this concept that the Government argued in *Progressive* "that its national security interest . . . permits it to impress classification and censorship upon information originating in the public domain, if when drawn together, synthesized and collated, such information acquires the character of presenting immediate, direct and irreparable harm to the interests of the United States." (467 F. Supp., at 991).

While Judge Warren did not deal specifically with the "born classified" concept, his views on the public availability of the information contained in the Morland article presage his conclusion as to the need for its protection:

> The Court is convinced that the government has a right to classify certain sensitive documents to protect its national security. The problem is with the scope of the classification system.
>
> Defendants contend that the projected article merely contains data already in the public domain and readily available to any diligent seeker. They say other nations already have the same information or the opportunity to obtain it. How then, they argue, can they be in violation of 42 U.S.C. 2274(b) and 2280 which purport to authorize injunctive relief against one who would disclose restricted data "with reason to believe such data will be utilized to injure the United States or to secure an advantage to any foreign nation . . ."?
>
> Although the government states that some of the information is the public domain, it contends that much of the data is not, and that the Morland article contains a core of information that has never before been published. Furthermore, the government's position is that whether or not specific information is "in the public domain" or has been "declassified" at some point is not determinative. The government states that a court must look at the nature and context of prior disclosures and analyze what the practical impact of the prior disclosures are as contracted to that of the present revelation.
>
> The government feels that the mere fact that the author, Howard Morland, could prepare an article explaining the

[33] The current Department of Energy Classification of Information Manual declares in a note: "Although the Atomic Energy Act makes no specifications for classifying RD (Restricted Data) and FRD (Formerly Restricted Data) at more than one level, three levels of protection have been established for such information based on its sensitivity. The designations used to denote those levels are the same as those used for NSI (National Security Information)." DOE Order 5650.2 (Dec. 12, 1978) at p. II–3 Thus, executive order classification categories are translated into the realm of Restricted Data, so that information may be designated, for example, "RD–Secret." The manual stipulates that RD and FRD may be declassified only by the DOE Assistant Secretary for Defense Programs ("DP–1"), and that RD and FRD may be downgraded only by DP–1 or the Director of Classification.

> technical processes of thermonuclear weapons does not mean that those processes are available to everyone. They lay heavy emphasis on the argument that the danger lies in the exposition of certain concepts never heretofore disclosed in conjunction with one another.
>
> The court has grappled with this difficult problem and has read and studied the affidavits and other documents on file. After all this, the Court finds concepts within the article that it does not find in the public realm—concepts that are vital to the operation of the hydrogen bomb.
>
> Even if some of the information is in the public domain, due recognition must be given to the human skills and expertise involved in writing this article. The author needed sufficient expertise to recognize relevant, as opposed to irrelevant, information and to assimilate the information obtained. (467 F. Supp., at 993).

Thus, while the Government did not argue that Morland had access to classified information or that any classified material had been stolen, Judge Warren accepted the notion that the manner in which Morland compiled and analyzed the information was the determinant here, not the individual pieces of information themselves.

The magazine relied in part on a World War II espionage case to demonstrate that information in the public domain should not be the basis for either prosecution under 42 U.S.C. 2274 or for suppression under 42 U.S.C. 2280. In *United States* v. *Heine*, 151 F. 2d 813 (2d Cir. 1945), *cert. denied*, 328 U.S. 833 (1946), the defendant was charged under the predecessor statute of current 18 U.S.C. 794 with unlawfully disclosing information affecting national defense. The statute specifically proscribed the communication of such information "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." The court described the information which had allegedly been sent to Germany:

> The information which Heine collected was from various sources; ordinary magazines, books and newspapers; technical catalogues, handbooks and journals; correspondence with airplane manufacturers . . . talks with one or two employees in airplane factories; exhibits, and talks with attendants, at the World's Fair in New York in the summer of 1940. This material he condensed and arranged in his reports, so as to disclose in compressed form the kinds and numbers of the planes—military and commercial—which were being produced and which it was proposed to produce; the location and capacity of the factories; the number of their employees; and everything else, of which he could get hold, that would contribute to as full a conspectus as possible of the airplane industry. (at 815).

All of the information relayed "came from sources that were lawfully accessible to anyone who was willing to take the pains to find, sift and collate it." (Id.)

The Government in *Progressive* rejected arguments by the defendants that it was obligated under 42 U.S.C. 2274(b) to demonstrate that

the information at issue would in fact be used to injure the United States. And defense contentions that the data was in the public domain were also disputed:

> Nowhere in the public domain is there a correct description of the type of design used in United States Thermonuclear weapons. The Morland article goes far beyond any other publication in identifying the nature of the particular design used in thermonuclear weapons in the United States stockpile. Although a minor proportion of the Restricted Data in the article is available in unrelated and scattered public sources, the preponderance of the Restricted Data is not available to the public in this form. In sum, its publication would provide a more comprehensive, accurate, and detailed summary of the overall construction and operation of a thermonuclear weapon than any publication to date in the public literature. (Reply Brief For United States, at 6).

Courts have struggled with the question of when it may be said that information has "entered the public domain." In *Alfred A. Knopf, Inc.* v. *Colby*, 509 F.2d 1362 (4th Cir. 1975), *cert. denied*, 421 U.S. 992 (1975), it was held that classified information does not enter the public domain merely for having been "leaked," absent official declassification. "Rumours and speculations circulate and sometimes get into print. It is one thing for a reporter or author to speculate or guess that a thing may be so or even, quoting undisclosed sources, to say that it is so. The reading public is accustomed to treating reports from uncertain sources as being of uncertain reliability, but it would not be inclined to discredit reports of sensitive information revealed by an official of the United States in a position to know of what he spoke." (at 1370). "It is true that others may republish previously published material, but such republication by strangers to it lends no additional credence to it." (*Id.*), While exceptions to such rules were acknowledged, the court urged judicial caution in this area: "One may imagine situations in which information has been so widely circulated and is so generally believed to be true, that confirmation by one in a position to know would add nothing to its weight. However, appraisals of such situations by the judiciary would present a host of problems and obstacles." (at 1370–1371).

The Government relied on several Freedom of Information Act (5 U.S.C. 552) suits to demonstrate its contention that the atomic energy information in Morland's article was not, in fact, already in the public domain. In *Aspin* v. *United States Department of Defense*, 453 F. Supp. 520 (E.D. Wis. 1978) the court said "past release of confidential information should not bind the executive branch if at a later point in time it is determined that further release would jeopardize national security." (at 524, citing *Halperin* v. *Central Intelligence Agency*, 446 F. Supp. 661, 665–666 (D.D.C. 1978)). And in *Lesar* v. *United States Department of Justice*, 455 F. Supp. 921 (D.D.C. 1978) name deletions were challenged in a suit to gain access to investigative reports with respect to the assassination of Dr. Martin Luther King, Jr. The court said: "Plaintiff, who has been a student of the King and Kennedy assassinations, claims that because he believes he can identify many of the names deleted, these names are in

the public domain. This is fallacious. The fact that an expert can piece together identifying data does not make the identifications in question automatically part of the public domain." (at 925).

Whether or not a piece of information has entered the public domain has been a matter for case-by-case adjudication—the subject apparently not lending itself to the imposition of general rules when potentially dangerous national security information is at issue. The few cases specifically on point suggest that while official publication will likely place the information in the public domain, anything short of that will not unless public knowledge is so pervasive as to render classification meaningless. And public awareness of parts of the whole will not necessarily by interpreted as public knowledge of an assemblage of those parts. The issue is perhaps more conducive to judicial resolution when the data involved has undergone an orderly classification process. Under the atomic energy statutes however, as illustrated in *Progressive*, the "born classified" concept allows that step to be omitted and leaves only the subject matter itself for review.

In a footnote to its Statement of Points and Authorities to the District Court the Government stated: "The fact that some of the secret Restricited Data contained in the 'Article' may represent the original work product of defendant Morland would not change its status as secret Restricted Data. Congress was well aware of the need to treat such information as confidential, even though no formal action had yet been taken by the government to restrict its distribution. This concept, known as 'classified at birth,' was deemed necessary by Congress to ensure that sensitive information would not be divulged before the United States had the opportunity to assess its importance and take appropriate classification action. Accordingly, the prohibitions against disclosure of Restricted Data aply with equal force to information 'born classified.' " (at 4).

The magazine suggested in *Progressive* that this aspect of atomic energy law is void for its overbreadth, i.e., that the "born classified" concept prohibits constitutionally protected conduct: "In enacting the Atomic Energy Act of 1954, Congress went too far in restricting the free exchange of information, and the government in this case has gone too far in its attempt to apply that Act to restrict freedom of the press. In the Act Congress recognized the legitimate need to protect certain information dealing with atomic weapons and atomic energy. But it adopted the most restrictive, the most drastic means for accomplishing that goal. It placed everything within the definition of 'Restricted Data,' banning its communication, transmission, or disclosure regardless of its origin or general availability unless it has been specifically declassified." (Defendant's Memorandum Brief, at 34). In addition, the magazine argued that such a system creates a statutory scheme which is unconstitutional for its vagueness in that "fair notice" is not accorded the individual citizen regarding what is Restricted Data and what has been declassified. (*Id.*, at 40, citing *United States* v. *Hariss*, 347 U.S. 612, 617 (1954)).

While Judge Warren did not expressly address the "born classified" concept, it is certainly arguable that his opinion constitutes tacit acceptance of the principle. He found that "the statute in question is not vague or overboard." (467 F. Supp. at 994).

At the subcommittee hearings, press lawyer Floyd Abrams was asked if he would favor an amendment that would carve out information that is in the public domain and remove it from the coverage of the Atomic Energy Act. He replied:

> I would personally be in favor of such legislation so long as the definition of public domain were not the definition that the executive branch has frequently made, which requires a positive declassification by them, but instead relates to the degree of public knowledge of the information itself irrespective of where the knowledge comes from.[34]

In his testimony, Abrams said it seemed to him "constitutionally unacceptable and in any event senseless" to have a statute on the books allowing "that something which has been publicly revealed to the extent that The Progressive article has may still be the basis of a prosecution so long as the Government can prove some degree of intent." He continued:

> For one thing, and not the least of the problems of the statute, it cannot work. Material that is once public cannot effectively, let alone constitutionally, be later rebottled as a secret. If I have an idea and if I disclose it to a friend or this committee, the notion that the Government can say that my material is and always was restricted is, I submit, intolerable in a free society.[35]

6. The Subcommittee Hearings

Hearings in February, March and August 1980 on the classification of private ideas were hamstrung by the reticence or refusal of agency witnesses to give full particulars about the *Progressive* case. Subcommittee efforts to explore *Progressive* fully were hampered by protracted and inconclusive negotiations—which continued into September 1980—over modification of the protective order Judge Warren imposed in March 1979 on key documents in the case, and by the Justice Department's seemingly endless mulling of possible criminal prosecution of persons who may have leaked, written about or published information containing Restricted Data.

Here are two examples of restraints imposed on the subcommittee's inquiry:

1—At the March hearing, a Department of Energy witness declared:

> As I mentioned, the Criminal Division of the U.S. Department of Justice is currently conducting a preliminary criminal inquiry into possible violations of the Atomic Energy Act and other Federal statutes which may have been committed in connection with the Morland and Hansen matters. The DOE has provided and will continue to provide the Criminal Division with all information in its possession regarding possible criminal violations by DOE employees, contractor employees or others. In view of the pending inquiry, it would be highly inappropriate for the Department of Energy to comment further at this time.[36]

---

[34] In Hearings.
[35] Id.
[36] Testimony of Duane Sewell in Hearings.

Under questioning, DOE witnesses at times demurred, saying "Since the case is still going on, that is all I can say about it right now," or "Well, I am not in a position to discuss the merits of the pending case right now since it is pending in the Justice Department."

2—On April 22, the subcommittee chairman requested a Justice Department briefing on the *Progressive* case and the status of the Criminal Division inquiry. Assistant Attorney General Alan A. Parker replied on May 27:

> As the Subcommittee is aware, the *Progressive* case is still pending before the district court in Wisconsin and, as a result, public comment would not be proper at this time. In addition, the case is approaching a crucial stage in settlement negotiations. In light of the status and sensitivity of those discussions, comment publicly on the handling of the case should be deferred.[37]

In connection with possible criminal prosecution, Parker wrote, "the Criminal Division is still conducting its analysis of the materials in question. We anticipate, however, that this assessment will be completed in the next several weeks."

To overcome such restraints and complete its investigation, the subcommittee has amplified the record by posing written follow-up questions and requesting studies and supplemental information. In addition, staff has held on-site discussions and interviews with DOE and other agency officials.

The most edifying statement of Government policy in the hearing record—linking the "born classified" concept, international considerations and action against *The Progressive*—was made in the June 1980 DOE letter of submittal to the subcommittee of the Hewlett born-classified study.[38] The letter said:

> The Department wishes to emphasize . . . the key role of the "born-classified" concept in the classification programs of the successor agencies to the AEC, the Energy Research & Development Administration and the Department of Energy. The Department firmly believes that the concept is as vital to the protection of the national security today, in an era of nuclear proliferation and terrorism, as it was during the post-World War II period of its conception. The grave danger to the nation posed by the proliferation of nuclear weapons information has been more keenly recognized in the last few years than ever before. The Treaty on the Nonproliferation of Nuclear Weapons and the Nonproliferation Act of 1978 evidence clear Congressional and Executive Branch concern over the ever-spreading capability of national and subnational groups to produce or acquire nuclear weapons. Most recently, of course, the Executive Branch has demonstrated its strong policy against proliferation by its attempts to enjoin publication of weapon design information generated by private citizens in the *United States of America* v. *The Progressive, Inc., et al*, and *United States of America* v. *Independent*

[37] In Hearings.

[38] The Department of Energy explained it believes there is a powerful link between the born-classified concept and prevention of nuclear proliferation.

Berkeley Student Publishing Co., Inc. Although the Government's efforts were thwarted by publication of sensitive material by a third party which mooted the law suits, the Government was successful in achieving court enforcement of the Atomic Energy Act provisions regarding Restricted Data in both cases.[39]

While the Executive Branch's efforts to prevent publication of the Morland and Hansen material did not succeed because of unfortunate factual developments, the Department of Energy believes that the Atomic Energy Act served as an effective legal mechanism for achieving Executive Branch goals in the litigation. Therefore, we strongly believe that any major overhaul of the enforcement framework of the Act is unnecessary and could be counterproductive.[40]

Testimony by the leadoff witness, Representative Paul H. McCloskey, led to pointed questioning of Sewell's claim that the law had worked. Mr. McCloskey had testified:

Clearly, the law of 1954 is now illusory. The law purports to protect against the spread of nuclear information. In *The Progressive* case, the court ruled that the spread of such information was so dangerous as to justify that very narrow constitutional prohibition and prior restraint. Yet, on reflection if the Department of Energy states, and I think accurately, that there is no way they can review a private citizen's work product in advance without losing their ability to perform their basic job then there may be no governmental remedy to this situation.[41]

Questioning of Sewell and DOE Deputy General Counsel Eric Fygi by subcommittee members and Mr. McCloskey led to the following exchange:

Mr. McCloskey. Still, how do you go back to Dr. Sewell's testimony? Here you have a perfectly understandable series of events, but how does the Atomic Energy Act work in this case? It didn't work. It didn't suppress the information. In fact the Government was frustrated and in fact no law has been violated.

Mr. Sewell. Let me turn to Mr. Fygi.

Mr. Fygi. Let me respond that we have not conceded that no law has been violated.

Mr. McCloskey. Who do you feel violated the law? It is now March 1980. This information was published in September 1979.

Mr. Fygi. Well, I am not in a position to discuss the merits of the pending case right now since it is pending in the Justice Department.

The ringing assertion of success echoed the March testimony of Duane Sewell, DOE's Assistant Secretary for Defense Programs:

[39] In hearings.
[40] In hearings.
[41] In hearings.

Mr. McCLOSKEY. Let me stop you just at that point. Would it be fair to suggest that it is the threat of use of the law rather than the law itself which you find to be the key weapon in your armory at this point?

Mr. FYGI. That may very well be true in this case as in other cases.

Mr. McCLOSKEY. And by delaying the enforcement of the law, the attempted test of the law, by holding the threat available, you are trying to chill the scientists in this case and the individuals from further communication. When you say that, it may very well be the case that the threat of the enforcement is greater than the law itself, because if the law were tested you could not convict anybody. Doesn't that accurately describe the present situation?

Mr. FYGI. It may describe a result of consequences, but not any deliberate policy.

Mr. McCLOSKEY. Mr. Chairman, this is my problem because I am afraid that this hearing cannot really reach the ultimate fact until the Justice Department makes a determination, yes, we will prosecute, or no, we will not.

Mr. PREYER. I think we may well want to recall the witnesses after such a determination has been made. That might be the proper time to pursue some of these questions.[42]

The inventory of unanswered questions in the aftermath of the *Progressive* case includes the following:

(a) Why did the Government abandon its "no comment" policy on articles such as Morland's and authenticate his work by moving to suppress it?

(b) Did the Government wrongfully disclose classified information by releasing the *Progressive* case affidavits of Drs. Harold Brown, Secretray of Defense, and Jack Rosengren, consultant to DOE, both of whom are recognized nuclear weapons experts?

Secretary Brown affirmed that

> The information . . . contained in the Morland paper describes correctly, in general, the basic principles of the functioning of a thermonuclear weapon.

Consultant Rosengren declared under oath that

> The Morland article goes far beyond any other publication in identifying the nature of the particular design used in the thermonuclear weapons of the U.S. stockpile.

It is contrary to DOE security regulations for Government weapons experts to publicly confirm or deny the accuracy of any article describing nuclear weapons design that is, or may soon be, in the open literature. The Brown and Rosengren affidavits apparently should have been designated "Secret Restricted Data" as were many others filed in *Progressive*. Their release constituted a serious breach of security.[43]

[42] In hearings.

[43] This point is made and elaborated in statements submitted for the hearing record by Ray E. Kidder, Associate Division Leader, Theoretical Physics Division, Lawrence Livermore Laboratory (LLL); Hugh E. DeWitt, physicist, H Division, Physics Department, LLL; and jointly by G. E. Marsh, A. De Volpi, T. A. Postol and G. S. Stanford of the Argonne National Laboratory. See Hearings. (In reply to Oakland, Calif., newspaperman John Miller's question, DOE's Sewell wrote on Oct. 16, 1979, that DOE had determined in conjunction with the Justice Department that the Rosengren affidavit "was unclassified and could be filed as part of the public record in the Progressive case.")

(c) As a statutory and practical matter, to what extent can DOE overlook, choose to ignore or wink at dissemination of information classified as Restricted Data?

On April 25, 1979, four members of the professional staff at the Argonne National Laboratory wrote Senator John Glenn to ask for a congressional investigation of the Government's release of classified information in the *Progressive* case. The letter was subsequently classified and not declassified until March 19, 1980, the day before the subcommittee hearing on the case. Yet when Oakland Tribune reporter John Miller asked DOE's Sewell why the Argonne scientists' letter to Senator Glenn and a letter that Charles Hansen had written to Senator Charles Percy remained classified despite having been printed in their entirety in publications of national circulation, Sewell responded:

> The Department of Energy is no longer taking action to control the dissemination of the documents described in your letter.[44]

(d) Does DOE defer declassification in poltically sensitive situations to strengthen the case for investigation of possible criminal violations?

Livermore physicist Hugh DeWitt (see note 37) wrote three affidavits for the court in *Progressive*. On December 11, 1979, the Lawrence Livermore Laboratory (LLL), run by the University of California under DOE contract, began an administrative investigation of DeWitt's alleged violation of LLL employee conduct policies on the handling of classified information in two instances, the first involving classified information given as part of an affidavit in the Morland/*Progressive* litigation. A memorandum of January 16, 1980, from Robert Southworth, LLL Security Manager, to John Anderson, LLL Associate Director for Physics, labeled "In the Matter of Hugh DeWitt," explains and observes:

> Violations of the Atomic Energy Act are investigated by the FBI. The Laboratory is responsible to report such matters to the Department of Energy which, in turn, reports to the FBI. This procedure was followed.
>
> DOE/Washington reportedly has recently declassified the information DeWitt provided. This, in the view of some, makes it more difficult to sustain a successful prosecution, even though it does not alter the fact that the initial action was in violation of Federal law.[45]

7. The Progressive Case: Unfinished Business

The District Court decision in *Progressive* was mooted, and therefore never made final. Its precedential value is unclear. The decision was unreviewed. The Justice Department has not decided whether to prosecute anyone for criminal conduct. If Justice elects not to prosecute, the DOE could be left to tend a virtually unenforceable Atomic Energy Act.

Progressive prompted the subcommittee inquiry into the Government's ability to classify, restrict or assert ownership rights over privately generated data. Its findings cast doubt on the fitness and fair

[44] In hearings.
[45] In hearings.

ness of classification practices and procedures. As the April 1979 letter of the Argonne scientists (see text accompanying note 38) pointed out:

> If individuals are allowed to selectively classify and declassify information for the purpose of influencing public policy debate, it should be recognized that they are being given power to deprive the American people of information they need to intelligently chart their future. While governments obviously have legitimate classification needs, it is imperative that these powers be used responsibly or we risk destroying the democratic society we wish to preserve.

In the hearings, DOE witnesses noted there is no statutory prohibition on the mere possession of Restricted Data. They also said the matter of requiring prepublication review for private researchers who have not had access to Restricted Data is a particularly complex problem. In short, private citizens cannot be penalized for possessing it, nor can they be required—if they think they may possess it—to present the data for clearance.

E. THE INVENTION SECRECY INTERLOCK

Of the 3,500 invention secrecy orders in force today, the oldest, according to the Patent and Trademark Office, was issued in 1942 on a patent application filed in 1940 and is sponsored by the Department of Energy. Two other patent applications filed in 1942 are covered by DOE-sponsored secrecy orders which were issued, respectively, in 1942 and 1947.

DOE last year sponsored 1,117 secrecy order renewals. Of these, 924 were imposed on DOE or predecessor agency-generated inventions. Of the remainder, 117 were issued at the request of foreign governments under mutual security arrangements, and 76 were imposed on privately owned patent applications. In the years 1975 through 1979, DOE sponsored 197 new secrecy orders, 50 of them in 1977. Of the patent applications not owned by DOE on which renewals have been issued, the average life of a secrecy order is eight years for one requested by a foreign government and 11 years for one imposed on a privately owned application.[46]

Whatever void may exist outside the realm of Restricted Data and the territory staked out by the executive national security information system is filled by the Invention Secrecy Act. The result may fairly be described as a statutory and administrative patchwork by which DOE acquires, suppresses, controls or lays claim to virtually all the intellectual property its eye can see. Some examples:

1—DOE sponsors many secrecy orders on its own patent applications covering inventions that are not Restricted Data but contain national security information;[47]

2—DOE presently sponsors no secrecy orders on privately owned applications that do not contain Restricted Data;[48]

3—Rescission of a secrecy order imposed pursuant to the Invention Secrecy Act does not itself declassify the information contained in the patent application. In actual practice the sequence would be the re-

[46] Testimony of Eric J. Fygi in Hearings.
[47] Id.
[48] Id.

verse; the secrecy order would be rescinded only after an original determination has been made that the Restricted Data contained in the application no longer requires protection and may be publicly disseminated without undue risk to the common defense and security; [49]

4—DOE reads the Atomic Energy Act to mean there can be no such thing as a private proprietary interest in weapon design information; [50]

5—There is a domain of Restricted Data susceptible of patentable private ownership. Since the act forecloses from patentability only inventions "useful solely" in an atomic weapon or, where inventions have multiple uses, "to the extent that such invention" is useful in atomic weapons, it is possible to patent inventions that might contain Restricted Data not directly useful in atomic weapons. Patentable inventions would include those relating to nuclear vessel propulsion systems and the technology of enriching uranium or producing plutonium, for example; [51] and

6—Any person who makes any invention or discovery useful in the production or utilization of special nuclear material or atomic energy and does not file a patent application on it is required by the Atomic Energy Act to file a report with the DOE within six months containing a complete description of it. If a patent application is filed, the Commissioner of Patents is required to notify DOE and grant it access to the application—after which the DOE may request a secrecy order on the invention.

Thus do all intellectual property roads lead to the DOE. Here is a road map drawn by DOE Deputy General Counsel Eric J. Fygi:

DEPARTMENT OF ENERGY,
Washington, D.C., June 23, 1980.

Hon. RICHARDSON PREYER,
Chairman, Subcommittee on Information and Individual Rights, Committee on Government Operations, House of Representatives, Washington, D.C.

DEAR MR. CHAIRMAN: Your letter of April 28 raised a series of questions suggested by the Subcommittee's March 20 hearing on the Government's ability to classify or assert ownership rights over privately-generated information.

You observe correctly that Executive Order 12065 does not, by its terms, affect the provisions of the Invention Secrecy Act, 35 U.S.C. 181–188. That order nonetheless did, by expressly exempting privately-generated information from classification under the order, indicate that executive agencies should employ particular restraint in considering whether to impose restrictions that the law may permit—rather than require—over dissemination of privately-generated information.

The practice of this Department's predecessors appears to have been consistent with this policy. While the relevant files are neither organized nor indexed to facilitate retrieval of those of our patent files involving secrecy orders, the individuals who administer these matters have advised me of only one instance during the last 14 years in which this Department's predecessors sponsored a secrecy order on a

[49] Letter of June 23 from Eric J. Fygi to the subcommittee chairman, responding to questions raised by the March hearing.
[50] Fygi testimony in Hearings.
[51] Id.

privately-developed invention that did not contain Restricted Data. The circumstances of that case involved information bearing directly on the functions and responsibilities of this Department.

The next questions posed in your letter are difficult to address because they imply rules of general applicability that might be suggested by extremely infrequent occurrences. It does not appear to me, though, that the sponsorship of a secrecy order under 35 U.S.C. 181 necessarily entails the judgment that the information sought to be protected is perforce classified under the pertinent Executive Order. The legislative history of the Invention Secrecy Act, while rather sparse, suggests that secrecy orders were intended to be issued in a variety of circumstances not confined to the Executive Orders prescribing classification standards, such as inventions originating in foreign countries whose governments, of course, apply their own standards in determining what technical information requires protection from widespread dissemination. Nor do I believe that, by sponsoring a secrecy order under 35 U.S.C. 181, an agency necessarily is taking, in the Constitutional sense, a "proprietary" or a "property" interest in the patent application, even if the applicant is eligible for compensation under 35 U.S.C. 183. See *Farrand Optical Co.* v. *United States*, 325 F. 2d 328, 335–37 (2d Cir. 1963).

Normally this Department acquires a property interest, as that term is used in the Invention Secrecy Act, in an invention under the terms of the contracts under which the Department provides financial assistance for research and development activities. Such contract clauses reflect the statutory policy common to both the Atomic Energy Act and the Federal Nonnuclear Energy Research and Development Act that title to inventions conceived in the course of performing such contracts vests in the United States. Other means by which this Department could acquire such a property interest would include purchase of a license or an invention itself, or by exchanges of such rights made to settle litigation. These latter categories could include products of "nongovernment research and development" within the meaning of Executive Order 12065.

When the Patent Office refers to this Department a privately-owned patent application for review under the Invention Secrecy Act, the first—and in nearly every instance the only—matter considered is whether the application contains Restricted Data under the Atomic Energy Act. In every instance of a privately-owned application, save the one example I mentioned previously, that determination is dispositive of whether this Department will sponsor a secrecy order under the Invention Secrecy Act. The one example involved an invention that, while not containing Restricted Data, did have significance in the field of space nuc'ear power systems.

Your questions regarding the effects of rescission of a secrecy order require a brief explanation of the process whereby declassification decisions are made under the Atomic Energy Act. As you are aware, section 11y of the Atomic Energy Act, 42 U.S.C. 2014(y), defines Restricted Data, and elsewhere the Act prohibits disclosure of such information. The definition itself, though, excludes information otherwise within the statutory formulation but which the Secretary of this Department has concluded may be publicly disseminated without undue risk to the common defense and security.

As the statutory scheme suggests, that determination is highly judgmental and requires fine weighing of scientific and other policy considerations. In this Department the authority originally to declassify Restricted Data has not been delegated below the Assistant Secretary level.

When the original declassification decision has been made, subordinate officials within the Department are authorized to apply that decision to documents in the Department's custody. Such subsequent decisions are not so much "declassification" decisions as they are determinations that a given document contains information that previously was judged by the Assistant Secretary no longer to require protection as Restricted Data. The nature of such subsequent determinations is largely technical and scientific.

Once the Assistant Secretary has made such an original declassification decision, I doubt that it could be subsequently reconsidered and the class of information involved reclassified under the Atomic Energy Act. As I described above, the original declassification decision sets in train a process that can alter the status of thousands of documents, with the effect that the information originally declassified rather promptly can arrive in the public domain. The Atomic Energy Act itself is silent on any authority to reclassify as Restricted Data information previously and correctly declassified, and the factual consequences of an original declassification decision seem incompatible with any subsequent attempt to reclassify as Restricted Data the same information. These observations are directed, of course, to proper exercise of judgment and statutory authority to declassify by the officer empowered to make such decisions, and not to instances whereby through clerical or similar error a document containing Restricted Data that has never been originally declassified is nonetheless marked and treated as though it were unclassified.

Applying these principles to the particular questions you posed, first the rescission of any secrecy order imposed pursuant to the Invention Secrecy Act does not itself declassify the information contained in the patent application. In actual practice the sequence would be the reverse; that is, the secrecy order would be rescinded only after the original determination had been made that the Restricted Data contained in the application no longer requires protection and may be publicly disseminated without undue risk to the common defense and security. If the rescission of the secrecy order were made in conformity with a proper original declassification decision by the Assistant Secretary, then I doubt that the information in any application so declassified could be subsequently reclassified as Restricted Data. It would not appear possible, moreover, for the information contained in such an application to be so removed from the Restricted Data category but retain a classification as national security information under Executive Order 12065, for the Atomic Energy Act limits the circumstances in which former Restricted Data can retain its character as sensitive defense information. See 42 U.S.C. 2162(d), (e).

Finally, you request that I augment the remarks that I made during the hearing in which I observed that, while Congress in 1954 determined that nuclear weapon design information would not be susceptible of private ownership as intellectual property protected by the patent laws, closer compensation questions can arise in the context of

information which is Restricted Data but is not necessarily related to weapon design.

This distinction arises from the Atomic Energy Act itself. In addition to information concerning the design, manufacture or utilization of atomic weapons, section 11y of the Act includes in the definition of Restricted Data "all data" concerning the production of special nuclear material (elsewhere defined as plutonium, uranium enriched in its fissionable isotopes, and similar material), and the use of special nuclear material in the production of energy. See 42 U.S.C. 2014(y). Section 151 of the Act, however, forecloses from patentability only inventions "useful solely" in an atomic weapon or, as to inventions admitting of multiple uses, "to the extent that such invention" is useful in atomic weapons. See 42 U.S.C. 2181(a) (b). This approach continued the patentability of a variety of inventions that might contain Restricted Data not directly useful in atomic weapons. Examples of inventions containing Restricted Data but that are nonetheless patentable would include inventions relating to nuclear vessel propulsion systems and the technology of enriching uranium or producing plutonium.

This survey of our experience with Restricted Data and application of the Invention Secrecy Act does not suggest to me any clear direction in which the Congress might consider amending the Atomic Energy Act. On the contrary, both statutes appear, through the compensation provisions of the Invention Secrecy Act and the compensation and award authorities of the Atomic Energy Act, to provide the tools necessary to mitigate or avoid the adverse and possibly unfair economic consequences to patent applicants whose privately-developed inventions might include Restricted Data. Should any amendment to the Atomic Energy Act in this area be introduced, this Department would consider it carefully and I expect that our analysis of any such proposal would be more concrete than these responses to the general questions posed in your letter.

As you requested, I am enclosing a copy of the Trial Judge's opinion in *Radioptics, Inc.* v. *United States*, 204 USPQ 866 (1979), along with the decision of the Court of Claims adopting the Trial Judge's conclusion. I hope this information will be helpful to you and to the Subcommittee.

Sincerely,

ERIC J. FYGI,
Deputy General Counsel.

The two courses open to a person who makes "any invention or discovery useful in the production or utilization of special nuclear material or atomic energy" may not represent a real choice. If he files a patent application to secure an intellectual property right, he risks a DOE-sponsored secrecy order if it determines the application contains Restricted Data (the Invention Secrecy Act standard in these circumstances is that an order shall issue if, in the opinion of an agency head, disclosure of the invention "would be detrimental to the national security"). If he does not voluntarily file a patent application, it is mandatory that he report the invention to DOE. The latter course

spares him from a possible secrecy order, but exposes him to a DOE determination that the invention contains Restricted Data.

By filing a patent application the inventor bares his discovery to DOE. In April 1976, DOE's forerunner, the Energy Research and Development Administration, sent the Patent Office a "Patent Security Category Review List" to guide it in making applications available to ERDA under both the Invention Secrecy Act and the Atomic Energy Act.[52] Under "nuclear fission reactions" the list specifies:

1. All nuclear fission reactors utilized for:
   (a) Power,
   (b) Propulsion,
   (c) Thermal energy,
   (d) Isotope or neutron production,
   (e) Experimental purposes.

This will include components and the manufacture thereof such as fuel elements, cooling systems, pressure vessels, shielding, loading mechanisms, steam and power conversion systems, auxiliary systems and accessories, identified as having possible application in nuclear reactors.

Under "nuclear *fusion* reactions" it identifies:

1. Laser fusion,
2. Electron beam fusion,
3. Ion beam fusion,
4. Magnetically confined controlled thermonuclear reactions.

Under "isotope and/or radioactive source technology" it specifies:

5. Materials, apparatus and methods utilizing (including responsive to) radioactive sources in:
   (a) Life Sciences such as medicine (diagnostic and therapeutic), ecology, disease and pest control, animal husbandry, etc.
   (b) Industrial processes such as food processing, sterilization, polymer production, etc.
   (c) Investigations of the environment or the earth.

It also specifies lasers, "regardless of power or energy output indicated as having utilization in isotope separation, nuclear fission or nuclear fusion."

As noted, DOE is presently sponsoring 76 secrecy orders on privately owned patent applications. In answering the subcommittee's follow-up questions, DOE's Fygi wrote that, in the personal knowledge of those who administer invention secrecy, only once in the last 14 years did DOE's predecessors sponsor a secrecy order on a privately developed invention that did not contain Restricted Data.

In the hearings, Fygi testified, "There is substantial overlap in both the function and application of the Invention Secrecy Act and the Atomic Energy Act." For example, the Invention Secrecy Act established the right of a patent applicant subjected to a secrecy order to seek "just compensation" for damage caused by the order itself. There is no parallel provision in the Atomic Energy Act for compensation resulting from classification of an invention as Restricted Data, but it does provide for a Patent Compensation Board to consider applications for compensation, awards and royalties based upon

[52] Emphasis in original. The cover letter acknowledges that "it is within the exclusive authority of the Commissioner of Patents and Trademarks to determine" which patent applications fall within the definition of "useful in the production or utilization of special nuclear material or atomic energy." See letter and unclassified list in Hearings.

claims under the act. Fygi testified that the board has been given authority to consider claims based upon the Invention Secrecy Act, and explained:

> Since its inception, the Board has considered 40 applications. Thirty-eight of the 40 applications were for awards and just compensation under the Atomic Energy Act. Two applications of the 40 included claims for compensation because of PTO secrecy orders. In the first application, the Board found the claim without merit. In the second application, claims were made for compensation and award under Sections 151, 153 and 157 of the Atomic Energy Act of 1954, as well as under 35 USC 183. The claim was settled for $120,000, and all rights in and to the invention were assigned to the Government without stipulation of which of the several allegations were relevant to the settlement.[53]

The Invention Secrecy Act authorizes the Commissioner of Patents and Trademarks to withhold the patent grant, while the Atomic Energy Act precludes the grant of a patent for an invention "useful solely" in an atomic weapon and forecloses patent rights for any invention to the extent of its use in atomic weapons. In pertinent part (42 U.S.C. 2181), the act reads:

> (a) Denial of patent; revocation of prior patents
>
> No patent shall hereafter be granted for any invention or discovery which is useful solely in the utilization of special nuclear material or atomic energy in an atomic weapon. Any patent granted for any such invention or discovery is revoked, and just compensation shall be made therefor.
>
> (b) Denial of rights; revocation of prior rights
>
> No patent hereafter granted shall confer any rights with respect to any invention or discovery to the extent that such invention or discovery is used in the utilization of special nuclear material or atomic energy in atomic weapons. Any rights conferred by any patent heretofore granted for any invention or discovery are revoked to the extent that such invention or discovery is so used, and just compensation shall be made therefor.

In a recent case, the United States Court of Customs and Patent Appeals reversed a decision by the Patent and Trademark Office Board of Appeals affirming a patent examiner's rejection of an applicant's claims on the ground that they pertained to an invention useful solely in the utilization of atomic energy in an atomic weapon. The case involved Allen Brueckner's application serial No. 65,756, filed July 13, 1970, and entitled, "Fuel Pellets For Controlled Nuclear Fusion." In affirming the examiner's rejection, the board had concluded, "If appellant's invented *fuel configuration for laser fusion burn* is an atomic weapon, then 42 USC 2181 proscribes the granting of a patent on the invention." (emphasis in original.) However, the court reversed, explaining in its opinion:

[53] Testimony of Eric, J. Fygi in Hearings.

> Even assuming that appellant's invention meets the definition of "atomic weapon" in section 2014(d), it is necessary to determine whether the invention is "useful *solely*" (sic) in an atomic weapon. The record is clear, and the PTO does not argue to the contrary, that appellant's invention has nonweapon utility. Therefore, we hold that the restrictions of section 2181(a) are not applicable. (footnotes omitted.) [54]

It should be noted that Breuckner's application was originally classified as Restricted Data when filed, but was declassified in 1974,[55] and that the Department of Energy, in an amicus brief to the court, sided with Brueckner against the Patent Office. DOE argued that the legislative history shows that Congress intended inventions "useful solely" in weapons not to be patentable, while inventions having dual uses would be patentable to the extent of their nonweapon use.[56]

Brueckner argued on appeal, said the court, that the unclassified status (since 1974) of his application "demonstrates that the invention is not directed to weapons technology." His application passed through a patent-withheld stage, which was measured by its status as Restricted Data, and reached a patent-precluded stage, where it was rescued by the court. His case shows how the powers conveyed by the Invention Secrecy Act and the Atomic Energy Act interlock.

---

[54] *In Re Allen Brueckner,* U.S.C.C.P.A , No. 80–530. Decided June 26, 1980. (Keith Allen Brueckner of KMS Fusion, Inc., was one of the experts consulted by the study panel, assembled by Pacific-Sierra Research Corporation and chaired by Gordon Moe, that prepared the report, "A Study On (sic) Government Control Of ICF Research," submitted to DOE in April 1979.)

[55] A secrecy order was placed on Brueckner's application on Oct. 16, 1970, and rescinded on Oct. 9, 1974, in accordance with AEC Classification Guide CG–LF–2. (Although laser fusion was frequently discussed in the late 1960's, the crucial concepts, including implosion, were not classified by the AEC until 1972. See "Fusion Power By Laser Explosion," by Emmett, Nuckolls and Wood, Scientific American, Vol. 230, No. 6 (June 1974), p. 2 of offprint.)

[56] A Patent Office holding of unpatentability for nonweapon uses would apply as well to Government-owned inventions.

APPENDIX

The "Born-Classified" Concept in the U.S. Atomic Energy Commission

A HISTORICAL STUDY PREPARED FOR THE GOVERNMENT INFORMATION AND INDIVIDUAL RIGHTS SUBCOMMITTEE OF THE COMMITTEE ON GOVERNMENT OPERATIONS, HOUSE OF REPRESENTATIVES

(By Richard G. Hewlett, Chief Historian, U.S. Department of Energy, May 1980)

Throughout its existence from 1946 to 1975, the U.S. Atomic Energy Commission consistently relied upon the "born-classified" concept in administering its statutory authority to control the dissemination of classified information. Under this concept the Commission maintained that certain types of information were "born classified," whether the information was generated in an official government project or in the mind of a private citizen working in his own home.

ORIGINS

Although the Commission and its staff almost never used the words "born classified," the concept grew quite naturally out of the American experience in World War II. The atomic bomb project was one of the best kept secrets of the war. The day before the attack on Hiroshima in August 1945, most Americans had no idea that the federal government was developing the atomic bomb or that the Army Corps of Engineers had constructed a network of massive production plants and laboratories in a dozen states across the nation. Scarcely a score of civilian and military officials had formal access to the information generated in all parts of the Manhattan Project. Everything related to the project, including its very existence, was "born classified."[1]

In the weeks following the Hiroshima and Nagasaki raids, a general description of the organization and scientific principles used to produce the bomb did become public, but every technical specification of the process employed remained classified, including even the fundamental physical properties of the heavy elements. The enormous power of the atomic bomb, its dramatic role in bringing the war with Japan to an abrupt end, and the mystery surrounding its development all had a deep psychological effect on persons within the project and in the public at large. The terrible destructive capabilities of nuclear weapons suggested to outsiders that the "secret of the bomb" should be locked

[1] Richard G. Hewlett and Oscar E. Anderson, Jr., *The New World 1939–1946*, Vol. I of A History of the U.S. Atomic Energy Commission (University Park, Pa., Pennsylvania State University Press, 1962), pp. 227–29, 238–39.

away in a vault, where it would be "safe" from potential enemies. Scientists and others within the Manhattan Project rejected this simplistic and uninformed reaction. Realizing that the true situation was much more complex and dangerous than the general public believed, those on the inside were, if anything, ever more determined to see that the bomb and the nuclear technology that produced it were brought under strict international controls. The bomb was universally perceived as an extraordinary threat to civilization that demanded extraordinary controls.[2]

Within a matter of weeks after the raids on Japan, however, a second and largely conflicting concern arose. The War Department, both in drafting legislation for the postwar control of atomic energy and in administering the laboratories in the Manhattan Project, gave indications that the very rigid controls over the activities of scientists might be continued into the postwar period. Many of the nation's most prominent nuclear scientists spoke out against continued controls over basic research. As Enrico Fermi remarked: "Unless research is free and outside of control, the United States will lose its superiority in scientific pursuit." [3]

This concern for scientific freedom dominated the first draft of the atomic energy bill which Senator Brien McMahon introduced in the Senate on December 20, 1945. In stating the purposes of the legislation, the McMahon bill gave greatest emphasis to "fostering private research and development on a truly independent basis" and to "free dissemination of basic scientific information and for maximum liberality in dissemination of related technical information." Section 9 of the bill, entitled "Dissemination of Information," attempted to distinguish between scientific and related technical information by declaring that basic scientific data "shall include, in addition to theoretical knowledge of nuclear and other physics, chemistry, biology, and therapy, all results capable of accomplishment, as distinguished from the processes or techniques of accomplishing them." The latter would fall in the category of "related technical information." Under the bill the new Atomic Energy Commission would be authorized to restrict the dissemination of technical information in the interest of national security "within the meaning of the Espionage Act." [4]

Although the original McMahon bill reflected a liberal attitude on the dissemination of information, it took a very restrictive position on the control of fissionable materials and facilities utilizing them. Private ownership of all such materials and facilities was to be prohibited and all patents related to the use of fissionable materials were to be assigned to the Atomic Energy Commission with due compensation for the inventor.[5] Thus the McMahon bill would create an absolute government monopoly over the production and use of fissionable materials.

In almost four months of hearings and executive sessions on the bill, McMahon's Special Senate Commitee on Atomic Energy moved steadily toward a more conservative position on the dissemination of scientific and technical information than the scientists advocated. The

---

[2] *Ibid.*, pp. 406–07, 415–18, 421–27.
[3] *Ibid.*, pp. 428–33.
[4] The McMahon bill, S. 1717, was printed in Senate Special Committee on Atomic Energy, Atomic Energy Act of 1946. Hearings on S. 1717, Jan. 22–Apr. 4, 1946 (Washington: Government Printing Office), pp. 1–9. Hereafter cited as Senate Hearings.
[5] Secs. 5 and 10 of S. 1717. The New World, pp. 493–98.

members of the committee, to begin with, were themselves more conservative than the scientists and tended to be more concerned about the security of "the secret" than about scientific freedom. This predilection was reinforced by revelations in January and February 1946 of Soviet espionage activities focussed on atomic energy projects in the United States and Canada. The committee was also concerned about practical matters such as the inadequacy of the Espionage Act to protect sensitive technical information. Secretary of War Robert P. Patterson told the committee: "The Espionage Act does not clearly prohibit the transmission of military information orally or by personal written communication even by present or former government employees unless actual subversive intent can be shown; nor does it prohibit the communication of information of military value that is discovered or developed by private persons." [6]

The committee's revisions of the bill in April 1946 reflected a drift toward a greater reliance on security. The declaration of policy in Section 1(a) was amended to read: "Accordingly, it is hereby declared to be the policy of the people of the United States that, *subject at all times to the paramount objective of assuring the common defense and security*, the development and utilization of atomic energy shall, *so far as practicable*, be directed toward improving the public welfare, increasing the standard of living, strengthening free competition in private enterprise, and promoting world peace." The portions italicized above were added to the original bill and illustrate the new balance struck between security and scientific freedom.

In the same vein the title of Section 9 (now Section 10) of the bill was changed from "Dissemination of Information" to "Control of Information." The Committee also abandoned the attempt to distinguish between "basic scientific" and "related technical" information and deleted the declaration establishing free dissemination as the cardinal principle in information policy. Now the emphasis was on restriction, including in one draft the right of the Secretaries of War and Navy to prescribe additional regulations on information concerning military applications of atomic energy. In place of the unworkable distinction between "scientific" and "related technical" information, the committee decided to establish a special category of classified information to be called "Restricted Data" and to be defined as "all data concerning the manufacture or utilization of atomic weapons, the production of fissionable material, or the use of fissionable material in the production of power, but shall not include any data which the Commission from time to time determines may be published without adversely affecting the common defense and security." The definition recognized the existing situation—namely, that all information related to these aspects of nuclear technology was already classified and could be declassified only by positive action on the Commission's part. Here was the seed of the "born-classified" concept.[7]

From the perspective of the scientists the McMahon committee had changed the character of the bill by stressing the control rather than the dissemination of information. When compared with the even more conservative attitude in the House of Representatives, however, the

[6] Senate Hearings, pp. 86, 89, 404–06. The New World, p. 493.
[7] The New World, pp 512–14.

McMahon committee took on the role of a champion of the scientists' cause during the House debates. Charging that the bill represented a plot by liberals to give the "secret" of the bomb to the Soviet Union, conservatives introduced amendments to exclude military information from declassification, to institute the death penalty for the willful disclosure of Restricted Data with intent to injure the United States, to require a unanimous vote by the Commission for the removal of information from the Restricted Data category, and even to return the entire Manhattan Project to military control for five more years. Most of these amendments were defeated in floor debate or were removed by Members of the McMahon committee in the House-Senate conference, but the margin of victory was usually small. On one crucial motion to recommit in the House, the bill survived by only nine votes.[8]

The legislative history of the Atomic Energy Act of 1946 as it became law on August 1 [9] made clear that the sense of the Congress was far more on the side of tight control of atomic energy information than on the side of liberal dissemination. Atomic energy was a frightening and mysterious force to be locked away behind the security barriers of the government project. In 1946 it had no place in the every-day life of most Americans.

EMERGENCE OF THE CONCEPT

In the years from 1946 to 1960, the Atomic Energy Commission and its staff attempted to strike a workable balance between the two conflicting policy objectives set forth in the 1946 Act: On the one hand to protect the common defense and security by retaining as Restricted Data any information that might jeopardize the nation's monopoly of nuclear technology and the bomb; and on the other hand, to declassify as much basic scientific information as possible and to encourage scientific research on atomic energy.

Without ever using the term, the Commission adopted the "born classified" concept as a working assumption. Given the definition of Restricted Data in the Act, everything encompassed by it was automatically classified. This fact meant that virtually every one of the hundreds of thousands of documents generated in the wartime project would have to be reviewed before they could be declassified. Although the Commission recognized the magnitude of this problem from the time it took over the project from the Army in January 1947, it was more than a year before any substantial amount of information was moved out of the Restricted Data category and made available to the public.[10] The initial approach was to assign classification officers at each major site to consider declassification requests as they arose, and a committee of Senior Responsible Reviewers was establishd to assure some uniformity in their decisions. When scientists in the laboratories urged that all security restrictions on basic scientific data be removed, the Commission cautiously opened a few topics to unclassified investigation. These were at first limited to radiation instruments, particle accelerators, specific chemical processes, and medical research and health studies. Under further prodding by the scientists the Commis-

[8] *Ibid.*, pp. 521–30

[9] The Atomic Energy Act of 1946 (P.L. 585, 79th Cong., 60 Stat., 753–75; 42 U.S.C., 1801–19).

[10] Minutes, Commission Meeting 18, Jan. 2. 1947.

sion in August 1948 removed restrictions on all instrumentation, mathematics, and all aspects of research in the physical and biological sciences which did not involve the fission process, weapons, or the properties or characteristics of elements above atomic number 90. This restriction effectively prohibited unclassified work on uranium or plutonium or on the development of nuclear reactors.[11]

By 1953 pressures from private industry for access to nuclear technology, particularly on reactor development, had built up a general consensus for major revisions in the Atomic Energy Act of 1946. Following the lead of the Eisenhower Administration, the Commission cooperated with the Joint Committee on Atomic Energy in the Congress in drafting revisions, which eventually became an entirely new statute, the Atomic Energy Act of 1954.[12]

Although the portions of the law dealing with Restricted Data and information control were essentially unchanged, the 1954 Act did make provisions for private industry to have access to Restricted Data in specific categories when the private companies agreed to comply with the Commission's regulations on classification and security.[13] A limited number of companies had for many years had access to Restricted Data as Commission contractors, but here again the contract imposed the Commission's security and classification regulations on the company.

In taking great care to keep all research and development activities involving Restricted Data under Commission control either through contracts or access agreements, the Commission avoided the troubling problem of private generation of Restricted Data. All Restricted Data born classified in the 1950s was kept under the Commission's control. The Commission's legal staff, however, was aware of the potential problem. In the summer of 1947, the scope of the Restricted Data section of the Act had been discussed with the Department of Justice. The Attorney General in a formal letter to the Commission addressed what he called "the problem of censorship of 'off-project' development." There was "considerable indication," the Attorney General wrote, that Congress intended the section "to cover all aspects of atomic development, whether under government sponsorship or otherwise, and to prohibit the dissemination of information relating to any such activities." But the Attorney General admitted that application of the section to private activities was "not lacking in difficulties, and that all areas of doubt on the part of laymen could be removed by amending it," perhaps by adding the words "whatever the source of origin" of the information. The Commission sent the Attorney General's letter to the Joint Committee on Atomic Energy, but no further action was taken.[14]

As long as most access to Restricted Data by private companies was limited to power reactor technology, it was not likely that the troublesome issue of privately generated information would arise. The national security implications of power reactor technology were limited essentially to protecting American interests in the international com-

---

[11] Richard G. Hewlett and Francis Duncan, Atomic Shield, 1947–1952, Vol. II of A History of the U.S. Atomic Energy Commission (University Park, Pa., Pennsylvania State University Press, 1969), pp. 83, 247; Guide to Unclassified Areas of Research, undated; Sixth Report of the Committee of Senior Responsible Reviewers, April 1–3, 1948; Seventh Report, June 11–12, 1948; Ninth Report, Dec. 17–19, 1948; AEC Press Release SP–21T, Dec. 1950; GM Bulletin 151, Dec. 15, 1949.

[12] Atomic Energy Act of 1954 (Public Law 83–703, 68 Stat. 919, 42 U S.C. 2011–2020).

[13] Section 145(a).

[14] Tom C. Clark to David E. Lilienthal, July 21, 1947; Lilienthal to Bourke B. Hickenlooper, July 22, 1947.

petition for the power reactor market, which seemed likely to become significant within a decade. There was also the prestige factor in demonstrating the superiority of the free enterprise system as part of the Cold War against the Soviet Union. But in a rapidly developing technology, trade secrets were a wasting asset and their loss would not vitally threaten the safety and security of the nation.

In 1960 a more dangerous possibility arose when several American companies began exploring the idea of starting research and development on the gas centrifuge process for producing uranium 235, a prime material for nuclear weapons. The Commission could not dismiss these requests outright because much of the recent research which made the gas centrifuge attractive had been done by private companies in Western Europe. To exclude American companies would put them at an economic disadvantage at a time when United States foreign policy called for vigorous efforts to capture the international market in nuclear technology. At the same time the centrifuge posed a serious potential threat to national security. If the process should make uranium 235 available at less cost in small plants which could be easily concealed, the United States' primary objective of preventing the proliferation of nuclear weapons might be compromised.

A reasonable response to the industry request was to establish a new category of classified information within the Commission's access program. Then private companies could have access to classified information on centrifuge technology if they complied with the Commission's security and classification regulations. The staff proposed that, in exchange for an access permit, each company agree to make all technical data produced available to the Commission and to grant the government a nonexclusive, royalty-bearing license for use of any invention or discovery for government purposes. The staff noted, however, that "should a private firm not want access to AEC's restricted data in building a centrifuge, the limitations as to participation and AEC rights to information through controls or access permits would not apply." [15]

In June 1960 the Commission agreed in principle that gas centrifuge technology would be incorporated in its access permit regulations (10 C.F.R. Part 25) but there were second thoughts about limiting application of the regulation to companies seeking access to the Commission's Restricted Data. In November 1960 the staff proposed that the amended Part 25 apply "to all permits for access to centrifuge information, whether or not the permittee desires access to AEC 'Restricted Data' information." The staff admitted that under the existing access regulations, the Commission did "not require or take privately owned proprietary information or receive reports concerning the private activity," but the Commission's need for access to private information on the centrifuge made this exception necessary.[16]

Although neither the Commission nor the staff acknowledged the presence of the "born-classified" concept, it was an underlying thread throughout their deliberations. In the access regulations as they then

---

[16] "Role of Private Industry in Development of Gas Centrifuge Process." AEC 610/29, Nov. 5, 1960; Minutes, Commission Meeting 1672, Nov. 15, 1960.

[15] "Role of Private Industry in Deevlopment of Gas Centrifuge Process," AEC 610/20, June 3, 1960.

existed, the Commission's authority to impose classification and security controls rested in part on the granting of access to Restricted Data. But in the amendments designed to cover the gas centrifuge, the Commission was declaring that the security and classification regulations applied even if access to the Commission's Restricted Data was not involved. The Commission was not saying, but clearly implying, that private research on the centrifuge would inevitably result in the generation of Restricted Data, which in turn would subject the private company to the terms of the regulation.

The proposed regulation issued for public comment on December 13, 1960, did not make the point clear. When a number of companies commenting on the amendment questioned the need for classification and the propriety of requiring Commission rights to technical data, the Commission decided to introduce one cautious statement of clarification. The terms and conditions for access would apply "irrespective of whether access to the Commission's Restricted Data information is desired." With this amendment the revised Part 25 became effective on April 20, 1961.[17]

THE SCOPE OF STATUTORY AUTHORITY

For several years the Commission relied upon the amended Part 25 to control the dissemination of Restricted Data by private companies, but by the autumn of 1963 the Commission's classification staff was growing uneasy about the effectiveness of the regulation. A few companies had contracts abroad to develop and manufacture nuclear devices that seemed to fall outside the Restricted Data topics set forth in the access regulations. In some instances companies were developing devices for purposes clearly unrelated to nuclear technology but which would be useful in producing fissionable materials and nuclear weapons.

The easiest solution would have been to declassify these nonnuclear commercial applications and to overlook their potential use in classified activities. This approach, however, would endanger the national security by encouraging the proliferation of nuclear weapons. The staff also noted that many of the scientists and engineers who were developing these nonnuclear commercial applications had worked on classified Commission projects. To declassify these activities might encourage others to take their ideas to private industry and further accelerate proliferation of classified technology.

The alternative was "to make clear to the public that privately generated information *can* be Restricted Data and that dissemination by its originator is prohibited except as authorized by law." The staff suggested that Part 25 might be further amended to make it applicable only to Government-owned Restricted Data, and that a new regulation (Part 26) be drafted to cover Restricted Data generated by private companies or in foreign countries. Persons desiring to disseminate privately developed Restricted Data would have to apply to the Commission for a permit, which the Commission would grant if the action would not endanger the common defense and security.

[17] "Amendment of Access Permit Regulations In Connection With Gas Centrifuge Process," AEC 610/35, March 28, 1961. The amendment to Part 25 was published in the Federal Register on April 20, 1961. AEC Press Release D–95, April 19, 1961.

The proposal for a new regulation reopened the question of whether the Commission had adequate statutory authority in this area. In its preliminary justification the staff relied entirely on the definition of Restricted Data in Section 11(y) of the 1954 Act:

> The term "Restricted Data" means all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 142.

The staff argued that the scope of the Commission's authority rested entirely on the meaning of Section 11(y). The definition used the words "all data" without limitation. There was nothing in the legislative history of either the 1946 or the 1954 Act to suggest that private work was intended to be outside the definition. Although the Attorney General had favored a clarifying amendment in 1947, he had decided that the Justice Department would proceed on the interpretation that the term was applicable to private information.[18]

Reassured on the point of statutory authority, the staff proceeded to draft two amendments to the Commission's access regulations. The first was the new Part 26 which was now designed to assert Commission authority over Restricted Data not covered by Part 25. As then written, Part 25 excluded access to the Commission's Restricted Data on nuclear weapons, the gaseous diffusion process, or naval propulsion reactors. Originally this exclusion had been sufficient to forestall any significant private research in these highly sensitive areas. But evidence of growing private interest in these fields suggested that Part 25 was no longer fully sufficient.

The draft presented to the Commissioners in July 1964 made clear for the first time the agency's interpretation of its statutory authority: "The statutory definition is not limited to information within the scope of the definition that is generated or owned by the Commission or the Government. It includes also any information within the scope of the definition that is generated by any person even though he may never have been engaged in any Government atomic energy activity."

In the draft regulation, "Non-Part 25 Restricted Data" was defined as that not falling within the categories of Part 25: "(a) generated in privately sponsored work; (b) generated under Government contracts which permit such dissemination subject to security requirements; (c) owned by a Government contractor; and (d) of foreign origin."[19]

The second change proposed in the regulations was to remove gas centrifuge technology from Part 25. This proposal in effect would reverse the Commission's decision in 1960 to add gas centrifuge research to Part 25 on the grounds at that time that private companies were beginning to enter the field and that some control was needed over the Restricted Data generated. By 1964, however, the situation had changed. During the intervening years the Commission's own contractors had made so much progress in developing the gas centrifuge in

---

[18] G J. Keto to C. L. Marshall, Oct. 10, 1963; E. B. Tremmel to Marshall, Dec. 31, 1963; " 'Restricted Data' As Applied to Private Research and Development," AEC 809/77, Feb. 12, 1964; Minutes, Commission Meeting 2002 March 27, 1964.

[19] "Control of Private R&D," AEC 843/29, July 21, 1964.

comparison with the modest efforts of private industry that it now seemed prudent to cut off private access to the Commission's Restricted Data in this field. If the proposed amendments were adopted, private companies would have no access under Part 25 but would be able to continue their own research without Commission data under the more restrictive provisions of Part 26. These changes would expose to public consideration more starkly than ever before the Commission's contention that the broad definition of Restricted Data in Section 11 (y) gave the Commission authority to control privately generated Restricted Data even when the private company had no official tie by access permit or contract to the agency.[20]

PROPRIETARY RIGHTS

One question which the proposed Part 26 did not discuss was the potential impact of the regulation on proprietary rights of individuals. The scanty evidence available suggests that the question was avoided in the draft regulation but not ignored in discussions within the staff. One of the alternatives considered was to prohibit any private person from disseminating or receiving Restricted Data related to the gas centrifuge. The staff rejected this idea because it would result in "presentation, in the sharpest focus, of the basic legal question of whether affected individuals were being deprived of property rights without due process and compensation." [21] Perhaps this consideration was responsible for use of the clumsy term "Non-Part 25 Restricted Data" in the draft regulation rather than the more direct "Private Restricted Data."

Franklin N. Parks, who was the Commission's legal expert on Part 25, was concerned enough about the issue of private rights to research the subject. Parks concluded:

> The basic objective of Part 26 and the companion amendments to Parts 25 and 95 is to protect the common defense and security. To the extent that the regulations impinge on freedom of speech they would appear to be a reasonable exercise of sovereign power, as authorized by the Atomic Energy Act, in the interest of the common defense and security. *Schenck* v. *U.S.*, 249 U.S. 47.
>
> To the extent that the regulations impinge on the use of property or property rights they would appear to be a reasonable exercise of sovereign power, as authorized by the Atomic Energy Act, in the interest of the common defense and security and for which the U.S. Government would not be financially liable. *Horowitz* v. *U.S.*, 267 U.S. 458; *Borg-Warner* v. *U.S.*, 89 F. Supp. 1013.[22]

Rather than publish the proposed regulation in the Federal Register for public comment, the Commission chose first to submit it privately to the Atomic Industrial Forum, which represented the major electric utilities and equipment manufacturers in the nuclear industry. The Forum was able to provide friendly advice from the perspective of

---

[20] "Role of Private Industry in Development of Gas Centrifuge," AEC 610/46, Feb. 14, 1964.
[21] AEC 843/29, July 21, 1964, p. 10.
[22] Franklin N. Parks to Legal Files, March 23, 1965.

atomic energy. In commenting on the proposed regulation Forum officials raised practical rather than constitutional issues. There was special concern that, in order to obtain Commission permission to disseminate Restricted Data under Part 26, private companies would have to give the Commission a large amount of proprietary information. Industry experience had been that the Commission was not always successful in preventing the dissemination of such information to commercial competitors. The industry representatives also contended that the term "Non-Part 25 Restricted Data" was completely inadequate, and they suggested instead that the proposed rule should specify particular categories of information that would be subject to it.[23]

The revised version of Part 26 which the staff presented to the Commission in December 1964 met the Forum's criticisms point for point. The term "Private Restricted Data" replaced the ungainly "Non-Part 25 Restricted Data" and five categories of Restricted Data were defined in the regulation. Proprietary information was to be protected by a new section which recognized the patent system and required private companies to issue the government licenses for government use with payment of reasonable royalties. Once again the Commission sent the draft regulation to the Forum for comment. One member reported back to the Commission that "the Forum participants were very much pleased that the comments made on the earlier draft of this regulation had been adopted rather completely." [24]

THE ISSUE JOINED

The Commission's approval of the new version of Part 26 on March 26, 1965 was on the condition that the staff would discuss the question of legal authority with the Department of Justice. One June 4 Wayne Barrett in the Office of Legal Counsel at Justice told Parks that the Department was "not completely satisfied that the Atomic Energy Act (1) was applicable to Private Restricted Data and (2) authorized the issuance of the proposed regulation." Barrett observed that it would have been a drastic step for Congress to have placed controls over private Restricted Data; under the circumstances he would have expected to find a specific reference to this authority in Section 2 or 3 of the Act, where Congress spelled out the rationale for other domestic controls. He admitted that the definition of Restricted Data standing alone and the enforcement provisions in Sections 224 and 225 could be read as including Private Restricted Data, but in the absence of direct evidence of Congressional intent to take this drastic step, he doubted that Congress intended to give the Commission such sweeping authority.[25]

Barrett later set down his views more systematically in a draft letter to the Commission, which he sent to Parks on September 30, 1965. In the draft Barrett proceeded by examining each section of the Act on which the Commission claimed to rely for its authority over Private Restricted Data. The first was Section 141, which stated that "It shall

[23] Julius H. Rubin to Gerald Charnoff, Sept. 25, 1964. Summary of Review Discussion on Proposed New AEC Regulation," Sept. 23, 1964.

[24] "Control of Private Restricted Data," AEC 843/30, Dec 11, 1964; Minutes, Commission Meeting 2067, Dec. 18, 1964; J. F. Young, General Electric Co., to Commissioner James T. Ramey, Jan. 19, 1965; "Proposed Part 26, Dissemination of Private Restricted Data," AEC 843/35, Mar. 26, 1965; Notes, Information Meeting 466, Mar. 29, 1965.

[25] Parks to files, June 4, 1965.

be the policy of the Commission to control the dissemination and declassification of Restricted Data in such a manner as to assure the common defense and security." Barrett claimed that this was only a statement of policy and not a grant of power. Secondly, Barrett turned to Section 145(a), which required the "prospective contractor, or the prospective licensee" to agree "in writing not to permit any individual to have access to Restricted Data" until a security investigation of the individual had been completed. This provision, in Barrett's opinion, implied that in the absence of a contract or license, the Commission would be without power to control dissemination. Thirty, Barrett cited similar language in Section 145(b) ("nor shall the Commission permit any individual to have access to Restricted Data") to mean "shall not itself disclose" rather than "shall not permit anyone else to disclose." The limited purpose of Section 145(b) was confirmed, in Barrett's opinion, by contrasting "it to five other sections of the Act which prohibited other persons from doing certain things unless authorized by the Commission to do so.

Fourthly, Barrett interpreted Section 161(i) as limiting the Commission's authority over Restricted Data to that arising from a contractual relationship. He thought this limitation was clearly conveyed by the wording of the Section, which authorized the Commission to "prescribe such regulations or orders as it may deem necessary . . . to protect Restricted Data *received by any person in connection with any activity authorized pursuant to this Act.*" (Emphasis added.) Fifthly, Barrett held that the enforcement provisions in Sections 224 to 227 were designed to deal with treasonable conduct or conspiracies and thus were doubtful authority for Part 26.[26]

In his informal response to the Commission's General Counsel, Parks admitted that there was "substantial merit" in the arguments in Barrett's draft letter, but he thought Barrett had ignored the historical context in which the 1946 Act had been drafted. He recited the overriding public concern in 1945 to protect "the secret of the bomb" and the paramount objective in the 1946 Act of assuring at all times the common defense and security. In reviewing the legislative history of the Control of Information section of the McMahon bill, Parks contended that the policy statement (the equivalent of Section 141(a)), could not be considered in isolation but only in the context of all other provisions of the Information chapter (Sections 141 to 146 of the 1954 Act). Parks used this same "historic-organic whole" argument to refute Barrett's interpretation of Section 145. Thus Section 145(a) merely set forth one way in which the policy statement in Section 141 was to be carried out. Likewise in Section 145(b) Congress was prescribing investigation and clearance of individuals having access to Restricted Data as one means of implementing the policy statement in Section 141.

As for Barrett's argument that Section 161(i) constituted inadequate authority for the regulation, Parks stated that for that very reason the Commission had not based Part 26 on that section. Rather the proposed regulation would be issued under the authority of Section 161(p), the general authority to issue regulations to carry out the purposes of the Act. Parks noted that no criminal penalties were attached

---

[26] Barrett to Parks, Sept. 30, 1965, with draft letter attached.

to violations of this section while severe penalties could be incurred by violating Section 161(i). Parks had no argument with Barrett's appraisal of the enforcement sections (224–227). In summary, Parks did not refute Barrett's arguments in a strict sense but rather cast Part 26 in an historical context that seemed to place its legal authority in a better light.[27]

Early in 1966 Parks completed a memorandum which discussed in detail the Commission's authority to control dissemination of privately developed Restricted Data. The memorandum elaborated each of the arguments that Parks had presented earlier and quoted extensively from the Senate hearings on the McMahon bill in 1946 and before the Joint Committee on revision of the Act in 1954. The purpose was to show the relevance of the legislative history in interpreting the Commission's authority.[28]

The Commission sent the draft memorandum to the Department of Justice in March 1966 and, after a series of meetings with Parks and others, the Justice Department officials concluded that the proposed regulations would be adequate if they were revised to delete specific references to criminal sanctions in the event the regulations were violated. During the summer and fall of 1966 the staff considered a number of revisions and even the possibility of seeking clarifying legislation. In March 1967 the staff presented to the Commission a revised version of the 1965 proposal to amend Part 25 and issue the new Part 26. The most substantive change was to replace the citation of criminal sanctions in Section 227 with a reference to injunctive proceedings in Section 232.[29]

THE QUESTION OF CONSTITUTIONALITY

The publication of the proposed regulation gave the public an opportunity to submit comments.[30] Several groups spoke to the issues of statutory authority and constitutional requirements. The atomic energy committee of the New York City Bar Association submitted the most comprehensive analysis.[31] The association acknowledged the "born classified" feature of the statute to be unique. "No affirmative action is required to classify data as restricted; the data is 'born secret.' In all other areas of national defense secrets affirmative action by the responsible agency is required in order to classify information as secret or restricted; the data in all such other cases is 'born free.' "

The statute, however, observed the bar association, was silent as to whether "born secret" data included that generated by individuals with no access to government information and with no association with the government. All reports, testimony, and hearings on the 1946 and 1954 Acts were silent on this point. Although the Commission had insisted since 1947 that the statutory definition of Restriction Data was intended to reach privately generated information,

---

[27] Parks to Joseph F. Hennessey, Nov. 15, 1965.

[28] Parks to Hennessey, Feb. 28, 1966; Hennessey to Commissioners Ramey and Palfrey, March 3, 1966

[29] Hennessey to Leon Ulman, Acting Assistant Attorney General, March 21, 1966; Sidney Kingsley, Draft of Clarifying Legislation, Nov. 10, 1966; "Proposed Part 26." AEC 843/42, March 20, 1967.

[30] Minutes, Commission Meeting 2271, April 21, 1967; AEC Press Release K–104, May 2, 1967.

[31] Richard D. Kahn, chairman, committee on atomic energy, New York City Bar Association to Hennessey, June 14, 1967.

Congress had taken no action to confirm or reject the Commission's interpretation. "The possible control of private data was not a clearly identified issue before the Congress in 1946 and 1954 because the question of possible military significance of private data did not arise until important private research and development efforts were commenced—after the passage of the 1954 act."

After examining the sections of the Act cited by the Commission as authority for control of private data, the bar association concluded that "the Commission seems to base the proposed Regulations principally on authority implied by the fact that the definition of the term Restricted Data is not expressly limited to governmental data. Particularly in light of the legislative history of the term, it is indeed fragile support for such a significant limitation on the rights of private individuals."

Beyond the question of statutory authority, the bar association found the proposed regulation "unconstitutional substantively as an undue interference with the exercise of free speech as protected by the First Amendment, and the application of criminal sanctions to enforce the Regulations would be unconstitutional as a deprivation of liberty and property without due process of law, as prohibited by the Fifth Amendment." Free inquiry, expression, and publication of an individual's ideas were protected against government encroachment by prior restraint or by subsequent sanctions. Furthermore, the courts had established that the legislative branch could not infringe upon such basic freedoms unless there was a clear and present danger that a substantial public evil would result, and even then the government had to show that it acted in the narrowest, most discriminate, and clearly intended manner. The Commission's proposed regulations, in the association's opinion, failed to meet these requirements in all respects.

A Washington law firm, writing for a company which would be affected by the proposed regulation, declared without any explanation that the regulation was unconstitutional as a violation of the First and Fifth Amendments. The American Civil Liberties Union found the assertion of authority to control privately generated Restricted Data to be a prior restraint on the freedom of expression and contrary to the First Amendment.[32]

During the summer and fall of 1967 Parks and other Commission attorneys drafted revisions which were designed to meet these constitutional objections. An obvious approach was to sharpen the definitions of the kinds of information that would be covered by Part 26. Sharper definitions would answer the constitutional objections that the regulations were vague, but they also inevitably destroyed the "umbrella" effect of more general terminology. Members of the staff then began to voice criticisms that the sharper definitions left too many loopholes through which Restricted Data might escape to the public. There were also dozens of questions from the staff about the adequacy of language describing security and administrative procedures.[33]

[32] Eugene P. Foley to W. B. McCool, Secretary of the Commission, June 15, 1967; Lawrence Speiser, American Civil Liberties Union, to Secretary of the Commission, June 14, 1967. Comments were also received from the Atomic Industrial Forum, General Electric Co., Union Carbide Corporation, Allied Chemical Corporation, and Esso Research and Engineering Co. Most of the comments from these organizations were related to questions of practicality and administration of the regulation.

[33] J. A Waters to Parks, Sept. 1, 1967; Roland A. Anderson to Parks, Sept. 15, 1967; C. L. Marshall to Parks, undated but about Sept. 1, 1967.

One proposal that received considerable attention was to use no-fund contracts to control the dissemination of Private Restricted Data. The use of contracts would obviate the charge that the Commission's stautory authority to control such data was weak. No-fund contracts, it was argued, could also be tailor-made for each individual case, would provide better controls, and had been used effectively before the access permit system was established. Further study in the General Counsel's office, however, revealed flaws in all these claims. The legal staff could cite several sections of the proposed regulations that provided the Commission with more flexibility than the contract approach offered. The terms of a contract could be varied to meet individual circumstances, but the basis for variation would have to be objectively justified if the contract method was to avoid constitutional objections. The terms of the revised Part 26 gave the Commission the option to impose additional requirements in special cases, but the contract approach depended upon negotiation of mutually acceptable terms. Furthermore, the General Counsel maintained that a regulation requiring private individuals to enter into a contract would be "very unorthodox." "The governing process is usually conducted by regulation and order; the Government directs. Control by a process of negotiation seems an inappropriate method of governing." Controlling Restricted Data was seen by the Commission staff as a governmental function. The assurance of due proceess required basic equality of treatment. If there were to be no standards for contracts in the regulations, there could be no assurance of equal treatment, and the absence of adequate criteria could raise First Amendment problems. In short, the use of the contract approach to avoid challenges in terms of statutory authority could lead to constitutional objections.[34]

The revised regulations which the Commission issued for public comment in December 1967 reflected both the earlier public criticisms and staff suggestions. First, the Commission confirmed its previous conclusion that "Commission control of specifically defined areas of such information is consistent with the statute and the Constitution." Secondly, the regulation had been revised to answer the charge that the categories of Restricted Data defined in Part 25 were too broad and vague to be used as a basis for criminal sanctions. To avoid this constitutional problem, Part 25 would apply only to persons who had received or generated Restricted Data in a government-connected activity. Under the old version the regulation would have applied to any person generating information in the categories described, whether or not the work was based on information received from the government. Thirdly, the revised regulations clarified the fact that Subsection 161(p) of the Act was the authority for Part 26, thus removing the ties to criminal penalties.[35]

Public comment on the revised regulation, which was published in the Federal Register in December 1967, revealed that the staff's attempts to meet the earlier expressed reservations about statutory authority and constitutionality had not been fully answered. The Atomic

---

[34] J. F. Hennessey to J. T. Ramey, Oct. 31, 1967; Hennessey to the Commissioners, Nov. 1, 1967.

[35] "Revised Proposed Part 26. 'Dissemination of and Access to Private Restricted Data,'" AEC 843/62, Oct 14, 1967. Minutes, Commission Meeting 2298, Nov. 1, 1967; AEC Press Release K–287, Dec. 22, 1967.

Industrial Forum, which acknowledged the Commission's best efforts to reshape the regulation in response to public comment, was still troubled by the fact that 'express authority to issue such regulations is nowhere conferred in the Act." Given the extremely important and fundamental rights which the Commission's regulations would limit, . . . [we] would recommend that the Commission consider seeking legislation more clearly defining (and refining) its authority." [36] The New York City Bar Association remained unconvinced on both statutory and constitutional grounds. Harold P. Green, a law professor and former Commission attorney who had written several articles on the subject, conceded the Commission's statutory authority but questions their constitutionality and practicality. Several commentators still questioned the scope of information covered by Part 25 and thought the language of the regulation was too vague. Further staff attempts to meet these objections were reflected in still another revision of the proposed Part 26, which the Commissioners reviewed in January 1969. Even then the Commissioners were unconvinced, and the statutory and constitutional questions were referred once again to outside legal authorities for study.[37]

With this deferral, the five-year attempt to promulgate Part 26 ended. In 1969 the Commission was becoming involved in the larger and equally perplexing questions of how to transfer the government's huge uranium enrichment facilities to private industry and how to control isotope separation technology in general. Late in the year an entirely new problem arose when KMS Industries, Inc., a Michigan research group, consulted the Commission about research the company was doing on controlled thermonuclear reactions. KMS was already exploring the possibility of using high-power, short-pulsed lasers to irradiate pellets of thermonuclear material and heat them to temperatures sufficient to initiate a thermonuclear reaction. Because this research had potential applications in the design of thermonuclear weapons, the Commission once again found a situation in which a private company was producing information that was "born classified." [38]

The proposed Part 26 would have provided a mechanism for handling the KMS case and others involving the use of lasers to produce thermonuclear reactions, but Part 26 was never promulgated. Instead the Commission reverted to its practice in the 1950s of negotiating no-cost contracts to provide a legal basis for controlling the dissemination of Restricted Data.[39] No further significant changes in the Commission's classified information policy were attempted before the agency was abolished in 1975.

[36] J. B. Knotts, Jr., to Secretary, AEC, May 9, 1968.

[37] "Part 26—Dissemination of and Access to Private Restricted Data and Related Amendments to Parts 25 and 95," AEC 843/67, Nov. 20, 1968. This paper contains summaries of the public comments. Minutes, Commission Meeting 2357, Jan. 6, 1969.

[38] F. T. Hobbs to W B. McCool, Oct. 10, 1969; Keeve M. Siegel to Glenn T. Seaborg, Nov. 25, 1969, Jan. 16, 1970; "CTR: Research on Micro Explosions Using Thermonuclear Pellets," AEC 532/89, April 23, 1970.

[39] Roland A. Anderson to Jack DeMent, May 11, 1970; AEC Press Release 0–14, Feb. 14, 1971.

ADDITIONAL VIEWS OF HON. PAUL N. McCLOSKEY, JR.

I would add some thoughts on Section III of the Report relating to the Atomic Energy Act of 1954.

This report should be understood for what it is . . . only the first step on what will be a long and tortuous road towards solution of the serious uncertainty in the Act brought to light over a year ago in the *United States* v. *The Progressive, Inc.*, 467 F. Supp. 990 (W.D. Wis. 1979).

This first step does no more than lay out the chronological order of events which led to our current problem. We owe a great debt of gratitude to Chairman Richardson Preyer for compiling this record, but we now owe even a greater obligation to ourselves. We need to build on this Report and go forward and solve the problem itself. As George Washington University law professor Mary Cheh pointed out nearly a year ago.

> . . . given the unsatisfying conclusion of the *Progressive* litigation, it is *imperative* that Congress now confront the uncertainty it created when it first wrote a law with such sweeping yet ambiguous information control provisions."[1] (Emphasis added.)

It is indeed imperative that Congress now act. Uncertainty in the law may be acceptable when the freedoms and reputations of ordinary citizens are not endangered, but for over a year now the freedoms and reputations of ordinary citizens, and particularly honorable scientists have been endangered.

The problem lies in the "Born Secret" concept contained in the Atomic Energy Act of 1954. It has three elements: (1) the classification procedures and policies of the Department of Energy, (2) the ambiguity of the present law as it is being interpreted by the Energy and Justice Departments, and (3) increasing public dispersion of scientific data bearing on construction and use of weapons which can destroy mankind . . . scientists, lawyers and legislators included.

These factors have led to a situation whereby the Government is now depending on the threat of criminal prosecution to cow scientists, both government and private, into restraint in the communication of ideas, while conceding that if criminal prosecution were attempted, it would probably fail.

At stake is the ability of scientists, both inside and outside government, to communicate with each other and thus advance scientific knowledge. Balanced against this goal, which has historically been considered as a highly laudable one, looms our growing uneasiness, if not conviction, that controlled advancement of science in the fields of nuclear weaponry, biological warfare and perhaps other areas such as genetics can destroy the world.

[1] Mary M. Cheh, The George Washington Law Review, January 1980, p. 163, 210. Reprinted in full as attachment A hereto.

Clearly, a balance is required between advancing science and protecting the public against a too-easy creation or possession by terrorists of hydrogen bombs, nerve gas and laser weapons.

The balance struck in the 1954 Atomic Energy Act, however, is clearly no longer adequate.

The question now is whether Congress will have the heart, courage and perseverance to build on this Report and continue to search for a solution.

The situation created by the *Progressive* decision, handed down March 26, 1979, is this: Whenever an individual, public employee or private citizen, generates a new concept of nuclear weaponry, that concept is "Born Secret" and, under the law, becomes classified information upon creation due to the statutory definition of Restricted Data.

But only the government can classify.

And, only the government can declassify. But declassification is easily accomplished. It occurs when the Government publishes previously-classified information or permits one of its scientists to do so. It can occur merely by putting information on the shelves of a public library.

The relevant section of the Atomic Energy Act is Section 2014(11)(y) which defines restricted data . . . that which is prohibited from publication . . . as:

> *all* data concerning (1) design, manufacture, or utilization of atomic weapons: (2) the production of specific nuclear material; or (3) the use of special nuclear material in the production of energy, but shall *not* include data declassified or removed from the Restricted Data category pursuant to section 2162 of this title. (Emphasis added.)

The last phrase is crucial. Restricted data does not include data which the government has declassified, i.e., allowed to be published in the public domain.

A great deal has been published in the public domain in recent years, most of it by distinguished government scientists—men like Edward Teller, Ted Taylor and George Rathjens.

From that mass of published information, and following questioning of several government scientists, an astute but scientifically unlettered newspaper reporter, Howard Morland, prepared an article for publication in The Progressive Magazine. Morland contends that he had described nothing more than information which had lawfully been "removed from the 'Restricted Data' category" through information released into the public domain. The Court felt otherwise, finding that the article contained "concepts" not previously published.

The Cour's language focuses on a hard reality:

> Faced with a stark choice between upholding the right to continued life and the right to freedom of the press, most jurists would have no difficulty in opting for the chance to continue to breathe and function as they work to achieve perfect freedom of expression.

In effect, the court found that the threat to life represented by unrestricted publication of H-Bomb facts justified prior restraint of that publication.

During the court proceedings, a private citizen who was also an amateur nuclear weapons enthusiast reached the conclusion that the Department of Energy was managing its classification program improperly. This private citizen, Chuck Hansen, contended that DOE had permitted leading government scientists in years past to publish the basic concepts of nuclear weaponry, but was now applying a different standard to private citizens such as Howard Morland.

Hansen felt that any "concepts" presented by Morland were easily deducible from already-published data.

Hansen had sent an 18-page letter to three Members of Congress and several newspapers containing his views. When the government learned of the letter, the Department of Energy (DOE) classified it and the Justice Department sought to prohibit the Daily Californian from publishing it. However, the Madison Press Connection, on September 16, 1979, published Hansen's letter in its entirety, rendering moot the Progressive controversy, and causing the Justice Department to drop its lawsuit.

Hansen had done nothing more than any private citizen might have done in reading public journals and studying data available to the public.

At least seven other people during the past several years have sent communications relating to nuclear weaponry concepts which they believed, in good faith, to contain information which had been properly declassified, only to have it promptly classified by DOE.

For example, in May of 1978 Dmitri Rotow, a Harvard student, found in the Los Alamos Public Library a document called "Final Design Status of the TX–7" and proceeded to write a paper on its content. Subsequently his paper was classified by DOE. A year later, Rotow returned to the Library to research the public availability of information on nuclear weapons for the American Civil Liberties Union. He then discovered document number UCRL 4725 and made copies of it. A librarian observing his work discovered that the document had been wrongly declassified.

Drs. Postol, Marsh, Stanford and DeVolpi at the Argonne National Laboratory have also maintained that DOE is manipulating the classification procedures for political purposes.

On April 25, 1979, during the *Progressive* case, they wrote a letter to Senator John Glenn concerning alleged misuse of DOE's classification procedures. DOE then classified their letter. Significantly, DOE did not remove such classification until one day before the Government Operations Subcommittee held public hearings on the question in March 1980.

Two scientists at the Lawrence Livermore National Laboratory, Drs. Hugh DeWitt and Ray Kidder, sent a memo to the regents of the University of California concerning the declassification of the Inertial Confinement Fusion Program. DOE immediately classified their memo.

Note that nine reputable individuals, six government employees and three private citizens, have therefore been able to generate communications in good faith, believing them to contain already-published information which the government subsequently chose to classify.

The six government employees all believed that DOE had used its classification procedures for political purposes rather than in checking bona fide attempts to protect nuclear secrecy.

What was the result? For months DOE and the Justice Department hinted darkly at possible criminal prosecution of the scientists. Finally, on September 4, 1980, Justice conceded that it would not prosecute.

The Ranking Republican Member of the House Armed Services Committee had previously criticized Justice for not enforcing the law.

Congressman Wilson wrote, on January 31, 1980:

> Notwithstanding the adequacy of existing laws, to prevent or deter the spread of Restricted Data, there has seen a reluctance by the FBI and the Department of Justice to aggressively investigate and prosecute alleged violations. Without enforcement no amendment to the law should make any difference.

Congressman Wilson's view was shared by top DOE officials who claimed that the FBI and Department of Justice have been remiss in meeting their responsibilities under the 1954 Act. DOE apparently felt that Morland, Hansen and Rotow, at least, could not have derived their new concepts had not someone at DOE "leaked" information. Both the Department of Justice and the FBI, at the congressional hearings in March 1980, indicated that they held little hope of successfully prosecuting private citizens under the 1954 Act, since to be guilty of any offense the private citizen would have to be proven guilty beyond a reasonable doubt, in the unanimous view of twelve fellow citizens that he published his ideas "with intent to injure the United States, . . . or with reason to believe such data will be utilized to injure the United States." (42 U.S.C. § 2274.)

As a former prosecutor and defense attorney, I agree completely. The chilling effect on government scientists is far more deadly, however. A government scientist can be prosecuted if he "knowingly communicates, or conspires to communicate or to receive, any Restricted Data, to any person not authorized to receive Restricted Data, or *having reason to believe* that such data is Restricted Data, to any person not authorized to receive Restricted Data . . . upon conviction thereof, be publishable by a fine not more than $2,500." (42 U.S.C. § 2277.) (Emphasis added.)

At the Subcommittee's hearings on March 20, 1980, DOE argued that the law might have been violated, and that the threat of prosecution was part of their policy. Note the following exchange:

> Mr. McCLOSKEY. Still, how do you go back to Dr. Sewell's testimony? Here you have a perfectly understandable series of events, but how does the Atomic Energy Act work in this case? It didn't work. It didn't suppress the information. In fact the government was frustrated and in fact no law has been violated.
>
> Mr. SEWELL. Let me turn to Mr. Fygi.
>
> Mr. FYGI. (Deputy General Counsel, DOE). Let me respond that we have not conceded that no law has been violated.
>
> Mr. McCLOSKEY. Who do you feel violated the law? It is now March, 1980. This information was published in September, 1979.
>
> Mr. FYGI. Well, I am not in a position to discuss the merits of the pending case right now since it is pending in the Justice Department.

Mr. McCLOSKEY. Let me stop you just at that point. Would it be fair to suggest that it is the threat of use of the law rather than the law itself which you find to be the key weapon in your armory at this point?

Mr. FYGI. That may very well be true in this case as in other cases.

Mr. McCLOSKEY. And by delaying the enforcement of the law, the attempted test of the law, by holding the threat available, you are trying to chill the scientists in this case and the individuals from further communication. When you say that it may very well be the case that the threat of the enforcement is greater than the law itself, because if the law were tested you could not convict anybody, doesn't that accurately describe the present situation?

Mr. FYGI. It may describe a result of consequence, but not any deliberate policy.

It was not until September 4, 1980, nearly a year and a half after the *Progressive* decision, that DOE and Justice finally conceded that neither the scientists nor the private citizens involved in the *Progressive* case would be prosecuted.

Under these circumstances, we have the unusual circumstances of DOE threatening its own scientists with the black cloud of dishonor and criminal prosecution, not because the law is clear, but because it is unclear!

This is, in effect, a rule of men, not of law. Respect for the law has never been more necessary, but that respect traditionally has been based on the premise that the law is clear and unambiguous and everyone is presumed to understand it. The law should not be a tool whereby an embarrassed bureaucrat can threaten an honorable employee in order to cover his own political headquarters.

As Professor Cheh said, it is imperative that Congress now act.

Both DOE's position and Justices position endanger the United States since those positions will clearly encourage the best scientists of the future to remain in private life rather than serve the government and risk irreparable damage to their reputations.

Also, if a Harvard student, a newspaper reporter and untrained nuclear amateur can generate articles gathered from publicly available sources, which the government feels must be kept secret because those articles threaten the peace of the world, the law is no longer adequate to protect the national security.

What is presently needed is a continuance of the hearings initiated by the Committee, inviting the leading members of the U.S. scientific community (and their lawyers) to come forward with specific recommendations. We clearly need a new law setting out a new balanace between the communication of scientific concepts and the protection against every American being able to add a nuclear weapon to his handgun collection. What that balance should be is clearly beyond the comprehension, will or desire of the lawyers of DOE and the Justice Department. It can only be resolved by Congress.

In order to focus the debate, I have introduced a bill,[2] the concept of which has been proposed by Mr. DeVolpi, and which would do two things:

(a) change the definition of "restricted data to omit lawfully published data or that which is derived from such data, thus allowing private citizens to act without fear of prosecution as regards any information lawfully published;

(b) requires that if private citizens are to be punished for violations of the Act, they have a specific intent to injure the United States or help a foreign nation, and are not subject to prosecution merely because DOE thinks they should have "reason to believe" they will harm the United States or help a foreign nation.

I am hopeful that this bill and this Report will serve as basic source documents for joint hearings early in the 97th Congress by the Subcommittee on Government Information and Individual Rights of the Government Operations Committee and the appropriate Subcommittee of Jurisdiction of the House Armed Services Committee. Perhaps the new Reagan Administration can force what the Carter Administration could not: a compromise between the Justice and Energy Departments as to whether this amendment or some other amendment to the 1954 Act will best serve the national interest under the new circumstances of the 1980's. Obviously some amendment should be a priority effort of the Congress in 1981. We owe this to our scientific community and to our national security.

PAUL N. MCCLOSKEY, Jr.

---

[2] A copy of this bill is appended as attachment B hereto.

ATTACHMENT A

THE PROGRESSIVE CASE AND THE ATOMIC ENERGY ACT: WAKING TO THE DANGERS OF GOVERNMENT INFORMATION CONTROLS.

MARY M. CHEH

Reprinted from
THE GEORGE WASHINGTON LAW REVIEW
Volume 48, Number 2, January 1980

The *Progressive* Case and the Atomic Energy Act: Waking to the Dangers of Government Information Controls.

MARY M. CHEH*

I. Introduction

The Atomic Energy Act (the Act) has been with us since 1946.[1] No law passed before or since gives the government such sweeping authority to keep information secret. Under the information control provisions of the Act, practically all information related to nuclear weapons and nuclear energy is "born classified": it is a government secret as soon as it comes into existence.[2] No governmental act is necessary to classify the information.[3] Moreover, the information, defined as Restricted Data, remains secret until the government affirmatively determines that it may be published.[4]

* Associate Professor of Law, The National Law Center, George Washington University; B.A. 1972, J.D. 1975, Rutgers — The State University (Douglass College); L.L.M. 1977, Harvard University. The author wishes to thank Mr. Harry Chernoff, B.A. 1977, William & Mary, who writes and works in the field of energy economics, for his assistance with various footnotes explaining the processes of fission and fusion and Mr. David Bamberger, 2d year law student, The National Law Center, George Washington University, for his assistance with footnote form and citation.

1. Atomic Energy Act of 1946, ch. 724, §§ 1-21, 60 Stat. 755 (current version at 42 U.S.C. §§ 2011-2296 (1976)).

2. 42 U.S.C. §§ 2014(y), 2162 (1976). The statute does not use the term "born classified"; this term is merely descriptive of the statute's operation. *See* notes 61-64 *infra* and accompanying text.

3. 42 U.S.C. §§ 2014(y), 2162 (1976). *See* notes 61-64 *infra* and accompanying text.

4. 42 U.S.C. §§ 2014(y), 2162 (1976). *See* notes 61-64 *infra* and accompanying text.

A question latent in the language of the Act is whether privately developed or privately generated atomic energy information — information developed or generated without government funds and without access to classified government documents — is Restricted Data and thus subject to the Act.[5] If it is, a scientist in a university laboratory, a researcher in a private industrial plant, or an enterprising journalist in the public libraries can independently compile, develop, or invent Restricted Data. Communication of this "secret" information contrary to the provisions of the Act consequently may be enjoined or may lead to a fine or imprisonment.[6]

The Atomic Energy Commission (AEC), now the Nuclear Regulatory Commission (NRC), and the Energy Research and Development section of the Department of Energy (DOE)[7] always assumed that the statutory definition of Restricted Data was broad enough to permit them to control any information falling within that definition, whether it originated within the government or elsewhere.[8] Until recently, however, the government had never pressed this view in

5. This article will not discuss the scope of the government's authority to impose secrecy on its own information. Such secrecy has long been accepted as a necessary corollary to the effective and efficient discharge of governmental responsibilities, particularly in the military and diplomatic spheres. Of course, a strong argument can be made that the public has a first amendment right of access to government information. *See* Emerson, *Legal Foundations of the Right to Know*, 1976 WASH. U.L.Q. 1. Until recently, the Supreme Court has rejected such a view. *See, e.g.,* Houchins v. KQED, Inc., 438 U.S. 1, 14 (1978). The rejection has come, however, primarily in the context of the media seeking access to prisons and prisoners. Last term, however, the Court found a first amendment right of access to criminal trials. *See* Richmond Newspapers, Inc. v. Virginia, 48 U.S.L.W. 5008, 5014 (U.S. July 2, 1980). It remains to be seen whether *Richmond Newspapers* signifies recognition of a general first amendment right of access to other traditionally public institutions. Congress has, by statute, granted a limited right of access to governmental information. The Freedom of Information Act, 5 U.S.C. § 552 (Supp. II 1978).

6. 42 U.S.C. §§ 2274, 2277, 2280 (1976). *See* notes 72-74 *infra* and accompanying text.

7. The Atomic Energy Commission (AEC) was created in 1946. Act of Aug. 1, 1946, § 2, 42 U.S.C. § 2031 (1970) (original version at ch. 724, § 2, 60 Stat. 756) (repealed 1974). In 1974, it was divided into the Nuclear Regulatory Commission (NRC), 42 U.S.C. § 5841(a) (1976), which took over the AEC's regulatory functions overseeing the nuclear power industry, 42 U.S.C. § 5842 (1976), and the Energy Research and Development Administration (ERDA), 42 U.S.C. § 5811 (1976), which assumed the AEC's research and development responsibilities, 42 U.S.C. § 5813 (1976). In addition, ERDA brought together programs from the Interior Department, the National Science Foundation, and the Environmental Protection Agency. In 1977, Congress passed President Carter's request for a new Cabinet-level Department of Energy. 42 U.S.C. § 7131 (1976). This department was given all powers then held by the Federal Power Commission (FPC), the Federal Energy Administration (FEA — a hybrid created in 1974, composed largely of the Federal Energy Office and several Interior Department offices), and ERDA. Those three agencies were thereby abolished. Dept. of Energy Organization Act, Pub. L. No. 95-91, 91 Stat. 582, 42 U.S.C. §§ 7301-7352 (Supp. I 1977).

8. For example, in 1967 the AEC prepared an internal memorandum entitled "Authority to Control Dissemination of Private Restricted Data" in support of proposed but never adopted regulations applicable to privately developed atomic energy information in four specific categories. *See* note 118 *infra*. *See also An Act to Combat International Terrorism: Hearings on S. 2236 Before the Committee on Governmental Affairs,* 95th Cong., 2d Sess. 281-83 (1978) (testimony of Donald Kerr, Acting Assistant Secretary for Defense Programs, Department of Energy) (hereinafter cited as *Hearings on S. 2236*); *Hearings before a Subcomm. on Reorganization of the Senate Comm. on Government Operations on S.J. Res. 21 to Establish a Commission on Government Security,* 84th Cong., 1st Sess. 268-70 (1955) (testimony of William Mitchell, General Counsel of the Atomic Energy Commission) (hereinafter cited as *Hearings on S.J. Res. 21*).

During the hearings on S. 2236, Senator Glenn questioned a DOE official on a central

court. In *United States v. The Progressive, Inc.*,[9] DOE invoked the information control provisions of the Atomic Energy Act and successfully enjoined a small but highly respected monthly news magazine[10] from publishing an article about government secrecy and the proliferation of thermonuclear weapons.[11] Entitled *The H Bomb Secret: How We Got It, Why We're Telling It*, the article contained information describing the theory and design of a hydrogen bomb.[12] Although all of the information in the article was based on private

---

issue addressed in this article, whether and to what extent the Atomic Energy Act applies to privately generated atomic energy information:

> Sen. Glenn: . . . How do you make your judgments in the aggregate on what are unclassified component parts? Is there a situation . . . that information drawn from public records or public sources is then put together in such a way as to become classified? How do you make a decision like that?
>
> I am thinking of this situation . . . [in which] all the material came from individually unclassified parts. How do you make a judgment on that?
>
> Mr. Kerr: . . .The first nuclear weapons were developed using unclassified principles of physics. What we are really concerned with is the assembly of information into a confirmed working design. Those parts that go with such a confirmed design are restricted data and protected as such, as are the detailed drawings and fabrication techniques for making them.
>
> Sen. Glenn: What rights would an author retain in a work that he developed from public sources but which later became classified?
>
> Mr. Kerr: If it were restricted data, he would have no rights to publish it and disseminate it unless it were within the classification system.
>
> . . . .
>
> With respect to materials that are already in the public domain, which have been distributed to libraries and which have been duplicated in part through other countries' publications in the same technologies as part of their reactor programs, I don't think there are acceptable and practical means restrictions on access to this information.

Hearings on S. 2236, supra, at 282- 83.

9. 467 F. Supp. 990, 1000 (W.D. Wis. 1979).

10. *The Progressive* is a monthly magazine with a nationwide circulation of about 40,000. It was founded in 1909 by Robert M. LaFollette, Sr. and, since that time, has established a national reputation for political commentary and analysis. *Id.*

11. 467 F. Supp. at 999. *The Progressive* promptly appealed the decision to the Seventh Circuit, which heard argument on September 10, 1979. Before the court of appeals announced a decision, a Wisconsin newspaper, the *Madison Press Connection*, published hydrogen bomb information so similar to that contained in *The Progressive* article that the case was effectively mooted. N.Y. Times, Sept. 18, 1979, at 1, col. 6. The information published in the *Madison Press Connection* was a letter written by a computer programmer and sent to Senator Charles H. Percy. *Id.* It included a wealth of technical detail on hydrogen bomb assembly, but had no relationship to *The Progressive* article. *Id.* After publication of the letter, the United States moved to lift the injunction against *The Progressive* and dismiss the case. *Id.* The government left open the possibility of bringing criminal charges against "anyone" for violation of the Atomic Energy Act. *Id. The Progressive* subsequently published the article in its November, 1979 issue.

12. THE PROGRESSIVE, May, 1979, at 14. While the *Progressive* case was still in litigation, few persons other than those associated with the proceedings read the article. *Id.* One day after the government commenced its action for an injunction, the trial judge issued a temporary restraining order preventing publication. *See* 467 F. Supp. at 991. On the same day, March 9, 1979, he also issued a protective order directing the defendants, their attorneys, and experts not to disclose anything contained in the article. *Id.* Significant portions of the record including the article and various affidavits were sealed. Nevertheless, it was publicly known that the article was approximately 18 manuscript pages in length and that it contained seven sketches hand-drawn by the author and captioned, *How a Hydrogen Bomb Works.* THE PROGRESSIVE, May, 1979, at 14.

research, interviews with government officials, and examination of documents placed in the public domain by the government,[13] the United States District Court for the Western District of Wisconsin concluded that it was Restricted Data that could not be published consistent with the Atomic Energy Act.[14]

Although seemingly predestined for Supreme Court review, the *Progressive* case was suddenly mooted by the publication of the same information in another newspaper.[15] The case nevertheless is important not only because it is the first case in which a prior restraint has been issued in the name of national security,[16] but also because it marks the first time the government has sought and obtained judicial imprimatur to extend security controls to private, non-

---

13. 467 F. Supp. at 993. The *Progressive* case did not involve the theft or compromise of any information possessed or owned by the government, *see, e.g.,* Rosenberg v. United States, 346 U.S. 273, 289 (1953), nor did it turn on the right of the government to protect its information by adopting a classification system or other security measures preventing its employees or agents from disclosing such information, *see, e.g.,* EPA v. Mink, 410 U.S. 73, 79 (1973); United States v. Marchetti, 466 F.2d 1309, 1318 (4th Cir.), *cert. denied,* 409 U.S. 1063 (1972). This article does not question the government's authority to protect information that it owns, possesses, or generates.

In this regard, Alexander Bickel perceptively observed that it is paradoxical to say that the government has a right to safeguard the confidentiality of its own information by keeping it secret at its source and by punishing those who steal or leak it and, at the same time, to say that the government has no authority, except in grave circumstances, to prevent someone from making the same information public regardless of how possession was obtained. He attributed the paradox to the attempt to reconcile two irreconcilable goals, privacy and public discourse, and the need for both in our system of government. The government may do all it can to protect information at its source, but the press, given its presumptive duty to publish, may do all it can to publicize the same information. A. BICKEL, THE MORALITY OF CONSENT 78-82 (1975). The point is that once the press or the public comes into possession of information, it is no part of the effective or legitimate operation of government to suppress that which by definition is not suppressible. An exception is made only if the information will lead to grave, immediate, and irreparable harm. *See* notes 234-36 *infra* and accompanying text.

14. 467 F. Supp. at 999. The trial court also rested its decision on the inherent authority of the President to protect national security, stating, "[i]n view of the showing of harm made by the United States, a preliminary injunction would be warranted even in the absence of statutory authorization. . . ." *Id.* at 1000. This article will not directly consider whether this inherent authority exists or, if it exists, whether it was properly exercised in this case. For a general discussion of such inherent executive authority, see Rubin, *Foreign Policy, Secrecy, and The First Amendment: The Pentagon Papers in Retrospect,* 17 HOW. L.J. 579 (1972); Junger, *Down Memory Lane: The Case of the Pentagon Papers,* 23 CASE W. RES. L. REV. 3 (1971); *The Supreme Court, 1970 Term,* 85 HAR. L. REV. 199 (1971).

15. *See* note 11 *supra.* The *Progressive* case is still pending but only with respect to whether and to what extent materials submitted by the parties should remain in camera under the trial court's original protective order of March 14, 1979. As part of its order vacating the preliminary injunction and dismissing the appeal, the Seventh Circuit remanded the issue of the continuing scope and applicability of the protective order to the trial court. United States v. The Progressive, Inc., No. 79-1428 (7th Cir., Oct. 1, 1979) (unpublished order).

In addition, while the *Progressive* case was on appeal, the government obtained a temporary restraining order against the intended publication of hydrogen bomb information by a California paper, *The Daily Californian.* The events leading to the dismissal of the case against *The Progressive*, *see* note 11 *supra*, also led to a dismissal of the case against the *Daily Californian.* N.Y. Times, Sept. 18, 1979, at 1, col. 6.

16. In June 1971, the United States did obtain national security temporary restraining orders preventing the publication of the Pentagon Papers, but the orders were dissolved by the Supreme Court within days. *See* New York Times Co. v. United States, 403 U.S. 713, 714 (1971) (per curiam). A chronology of the events leading to up the Supreme Court's decision can be found in M. SHAPIRO, THE PENTAGON PAPERS AND THE COURTS 1-16 (1972). *See also* S. UNGAR, THE PAPERS AND THE PAPERS (1972).

governmental, industrial, scientific, university, or journalistic activities.[17]

This article outlines the historical and legislative background of the Atomic Energy Act's controls over privately developed information, examines how these controls have been applied, and discusses whether they are justifiable as a matter of law or policy. A central inquiry is whether Congress, in enacting the Atomic Energy Act, intended to depart from customary classification practice and impose secrecy on non-governmental, privately developed information.

II. Overview

A. The Atomic Energy Acts of 1946 and 1954

Atomic energy information controls are one facet of comprehensive government regulation of all atomic energy activities. The first atomic energy legislation was the Atomic Energy Act of 1946.[18] It gave the government an absolute monopoly over all aspects of atomic energy research, development, and production.[19] Private enterprise was relegated to a relatively narrow ambit of permissible activity, and no patents were permitted for inventions or discoveries useful in the production or utilization of atomic weapons or fuels.[20] Information relating to atomic energy was called Restricted Data and, as such, classified as secret.[21]

From an historical perspective it is not surprising that the 1946 Act emphasized national security concerns. Nor is it surprising that security was thought to depend on absolute government control of atomic energy materials and maintenance of secrecy over atomic energy information. In 1946, atomic energy was still a relatively new and little understood force.[22] Only the atomic scientists and military personnel who had worked on the Manhattan project[23] had any depth of

17. The only statute that specifically permits the government to impose secrecy on privately developed information in the name of national security is the Invention Secrecy Act, 35 U.S.C. §§ 181-188 (1970). This Act applies, however, only to patent applications and then only in limited circumstances. The constitutionality of this law has never been directly challenged, but the Act has been impliedly upheld in litigation questioning whether it was properly applied. *See, e.g.*, Halpern v. United States, 258 F.2d 36, 38-39 (2d Cir. 1958).

18. Atomic Energy Act of 1946, ch. 724, §§ 1-21, 60 Stat. 755 (1946) (current version at 42 U.S.C. §§ 2011-2296 (1976)).

19. *Id.* §§ 3-7, 9-12, 42 U.S.C. §§ 2051-2135.

20. *Id.* § 11, 42 U.S.C. §§ 2181-2190.

21. *Id.* § 10, 42 U.S.C. §§ 2161-2166.

22. *See* R. HEWLETT & O. ANDERSON, JR., THE NEW WORLD xi-xii, 7-8 (1962); S. REP. No. 1325, 88th Cong., 2d Sess. 5, *reprinted in* [1964] U.S. CODE CONG. & AD. NEWS 3105, 3109.

23. The "Manhattan Engineer District" was the name given to the United States atomic bomb development project. Begun in 1942, the project enlisted the aid of scientists from around the world, employed 150,000 persons, cost approximately two billion dollars, and ultimately led to the discovery, construction, and detonation of an atomic bomb in 1945. *See* B. GOLDSCHMIDT, THE ATOMIC ADVENTURE 26 (1964). Despite the size of the project, secrecy was tight and the atomic bombing of Hiroshima on August 6, 1945, took the world almost completely by surprise.

understanding or sophistication about its problems and potential.[24] The public knew only that atomic energy was harnessed to make a bomb of unimaginable destructiveness and that the United States was the only nation with the "secret" of the bomb. The idea quickly developed that security and world stability turned on keeping other nations from learning our atomic energy "secrets."[25] Congress was not immune to these sentiments. Although atomic scientists had some success convincing legislators that secrecy was futile or actually inimical to security,[26] the final version of the Atomic Energy Act of 1946 strongly emphasized secrecy.

In the years following the passage of the 1946 Act two developments signaled a changed perspective. First, the Soviet Union joined the United States as an atomic power.[27] Second, the United States gave increasing attention to harnessing atomic energy for peaceful purposes.[28] Indeed, there was hope that atomic energy would provide an extremely inexpensive source of electricity.

Accordingly, in 1954, Congress substantially amended the 1946 Act. The new version of the law, renamed the Atomic Energy Act of 1954,[29] ended the government monopoly over the production and development of atomic energy by authorizing the participation of private enterprise in all atomic energy technologies, except weapons development.[30] It also relaxed patent restrictions[31] and authorized

---

24. *See* Miller, *A Law Is Passed — The Atomic Energy Act of 1946,* 15 U. CHI. L. REV. 799, 801 (1948).

25. *Id.* at 810.

26. *See, e.g., Hearings on H.R. 4280 Before the House Comm. On Military Affairs,* 79th Cong., 1st Sess. 80-82, 97-100, 118 (1945). The scientists argued that secrecy was futile because of the inevitability that other nations would learn the basic scientific information needed to make an atomic bomb. In addition, they insisted that secrecy would actually harm national security because it would retard scientific progress and thereby nullify the United States head start position. *Id.*

27. *See* Feld, *Nuclear Proliferation — Thirty Years After Hiroshima,* PHYSICS TODAY, July 1975, vol. 28, no.7, at 23. The Soviet Union successfully detonated an atomic bomb in September 1949. Great Britain followed three years later, in October 1952. The United States successfully detonated a *hydrogen* bomb in November 1952. The Soviet Union followed in August 1953, and Great Britain followed in May 1957. Currently five countries, the United States, the Soviet Union, Great Britain, France, and China, are known to have exploded a hydrogen bomb and an atomic bomb. India successfully exploded an atomic bomb once, in March 1974. *Id.*; Congress of the United States, Office of Technology Assessment, NUCLEAR PROLIFERATION AND SAFEGUARDS 93-111 (1977).

Although only six countries have successfully detonated nuclear weapons, roughly twenty are believed to be involved in some form of nuclear weapons development. Israel and Pakistan, for example, are believed to have the current capability of detonating an atomic bomb. *See* N.Y. Times, July 1, 1979, at A 21, col. 2 ; *id.*, Mar. 2, 1978, at A 5, col. 1. Experts in the Carter administration predicted recently that, within five years, Taiwan, South Korea, South Africa, Brazil, and Argentina would join the nuclear arms club. *Id.* Apr. 7, 1980, at A 1, col. 5. Some of these experts maintained that by 1990, Egypt, Libya, Iran, and Iraq could acquire the means to make nuclear weapons. *Id.*

28. *See* S. REP. NO. 1699, 83d Cong., 2d Sess. 2 *reprinted in* [1954] U.S. CODE CONG. & AD. NEWS 3456, 3457-58.

29. Atomic Energy Act of 1954, ch. 23, 68 Stat. 921 (codified at 42 U.S.C. §§ 2011-2296 (1976)). For a general discussion of the 1954 Act, see Green, *The Atomic Energy Information Access Permit Program,* 25 GEO. WASH. L. REV. 548, 548-52 (1957); SCIENTIFIC AMER., Nov. 1954, at 31.

30. Atomic Energy Act of 1954, §§ 31, 101-104, 42 U.S.C. §§ 2051, 2131-2134 (1976).

31. *Id.* §§ 151-153, 42 U.S.C. §§ 2181-2183 (1976).

cooperative agreements permitting the exchange of information with other nations.[32]

Creation of a viable private atomic energy industry necessarily meant easing the government's tight control over Restricted Data.[33] The 1954 Act did not, however, amend the definition of Restricted Data or materially change the information control provisions of the 1946 Act. Nor did it authorize declassification of information previously thought protective of national security. Rather, it broadened the class of persons to whom access to Restricted Data would be given. Under all other government programs, the 1946 Act included, access to classified information was[34] (and still is[35]) limited to government employees and to government contractors or licensees who demonstrated a "need to know"[36] the information. Under the 1954 Act, however, Congress provided a basis under which private entities licensed by the AEC to develop peaceful uses of nuclear energy, such as nuclear reactor licensees, could also be given access to Restricted Data.[37] Although this development meant that large numbers of persons not involved in government programs might be permitted to share in classified information, Congress apparently believed that security could be tightly maintained so long as all such persons were investigated, cleared, and made subject to criminal sanctions for violating security rules.[38]

Soon after the passage of the 1954 Act, the AEC, pursuant to section 3(b)'s exhortation to broadly disseminate Restricted Data "so as to encourage scientific and industrial progress,"[39] extended even further the class of persons to whom access to Restricted Data could be provided. Under the Access Permit Program,[40] the AEC provided access to Restricted Data to any person who could show a potential use for the information in his trade, business, or profession.[41] Thus, under the 1954 Act, large numbers of persons not involved in government programs were permitted to share in Restricted Data after obtaining appropriate security clearance and agreeing to adhere to all security controls.[42]

---

32. *Id.* §§ 121-124, 42 U.S.C. §§ 2151-2154 (1976).
33. *See* Ruebhausen & von Mehren, *The Atomic Energy Act and the Private Production of Atomic Power*, 66 HARV. L. REV. 1450, 1482-83 (1953).
34. *See, e.g.*, Exec. Order No. 10,501 § 7, 22 C.F.R. § 212 (1953).
35. Exec. Order No. 12,065 §§ 1-4, 3 C.F.R. §§ 190, 199 (1979).
36. *See* Green, *supra* note 29, at 550.
37. Atomic Energy Act of 1954, §§ 145(a), 145(f), 42 U.S.C. §§ 2165(a), 2165(g) (1976).
38. *See* Green, *Information Control and Atomic Power Development*, 21 LAW & CONTEMP. PROB. 91, 96 (1956).
39. Atomic Energy Act of 1954, § 3(b), 42 U.S.C. § 2013(b) (1976).
40. For a detailed discussion of the Access Permit Program, see Green, *supra* note 29, at 548-67. The program remains in operation today. *See* 10 C.F.R. App. A § 725.1 (1978) (describing the categories of information encompassed by the program).
41. 10 C.F.R. § 725.15 (1978).
42. *See* note 150 *infra*. *See generally* Green, note 38 *supra*.

B. The Information Control Provisions

The information control provisions have remained virtually unchanged since the 1946 Act. They remain keyed to the concept of Restricted Data defined as "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category . . . ."[43] Although this definition appears specific, it is fraught with imprecision, primarily because of the word "concerning", meaning "related to" or "about" atomic weapons or special nuclear material.

The Act defines an atomic weapon as "any device utilizing atomic energy . . . the principal purpose of which is for use as, or for development of a weapon, a weapon prototype, or a weapon test device."[44] Special nuclear material is "plutonium, uranium enriched in the isotope 233 or in the isotope 235 . . . or . . . any material artificially enriched"[45] by plutonium or uranium 233 or 235. Other component parts of the Restricted Data concept have a similarly broad sweep. The word "design," for example, includes "(1) specifications, plans, drawings, blueprints, and other items of like nature; (2) the information contained therein; or (3) the research and development data pertinent to the information contained therein,"[46] and "research and development," in turn, includes "(1) theoretical analysis, exploration, or experimentation; or (2) the extension of investigative findings and theories of a scientific or technical nature into practical application for experimental and demonstration purposes, including the experimental production and testing of models, devices, equipment, materials, and processes."[47] Informational sources such as a college class discussion in physics[48] or even the day-to-day reporting of the events

43. 42 U.S.C. § 2014(y) (1976).
44. *Id.* § 2014(d).
45. *Id.* § 2014(aa).
46. *Id.* § 2014(i).
47. *Id.* § 2014(x).
48. Testifying before the Joint Committee on Atomic Energy on the sweeping secrecy provisions of the Atomic Energy Act, atomic scientist and teacher Dr. Enrico Fermi stated:

> But this secrecy acts as a tremendous brake on progress. If I may give you an example. I am teaching a course in nuclear physics at the University of Chicago, and I would have liked to give my students certain background to the work in atomic energy.
>
> I have a fair notion of what is classified and what is not classified, but still the feeling that I would have had to weigh my words very carefully — I could have been asked embarrassing questions, and I would have been faced with the choice of either telling a student in the open classroom, "I am sorry, my boy, but this is something that I am not allowed to answer." And just this uneasiness drove me to stay off the subject. . . .
>
> Perhaps the belief is that in basic science much more is kept under wraps than actually is. But just the feeling of this blank wall — the fact that nobody knows exactly where the wall begins, how far one can go without overstepping the limits — acts as an extremely serious psychological block against what would be a very natural and very appropriate field for free investigation.

Hearings Before the Joint Comm. on Atomic Energy Pt. 21, 81st Cong., 1st Sess. 871 (1949) (testimony of Dr. Enrico Fermi). *See Hearings Before the Joint Comm. on Atomic Energy on Development, Growth and State of the Atomic Energy Industry*, 85th

surrounding the Three Mile Island reactor incident in March 1979[49] conceivably could fall within this expansive definition of Restricted Data. Given the breadth of the Restricted Data concept, it therefore is not surprising that one expert characterized the term Restricted Data as including "virtually all atomic energy information which the AEC believes warrants protection in the interest of security."[50]

During hearings on the Atomic Energy Act of 1954, at least one legislator expressed concern over the breadth of the Restricted Data definition, but his colleagues did not seem to share his sense of alarm.[51] Furthermore, even though by 1954 Restricted Data had found its way into the public domain without having been officially declassified, Congress made no effort to amend the definition of Restricted Data to reflect this reality.[52] The definition in the 1946 Act was simply reenacted in the 1954 Act with minor alterations.

Once information falls within the broad definition of Restricted Data, it becomes subject to statutory restrictions. First, dissemination of the information is controlled by rules and regulations governing its possession, transmission, and safekeeping, which the Act authorizes DOE and NRC to promulgate.[53] Second, access to or continued possession of the information is conditioned on obtaining a security clearance from the government.[54] Finally, unauthorized communication of the information may be enjoined or criminally punished.[55]

Currently, DOE and the NRC share the responsibility for safeguarding Restricted Data.[56] Their primary duty is "to assure the common defense and security,"[57] but, consistent with that objective, they

---

Cong., 1st Sess. 177 (1957) (testimony of V. Lawrence Parsegian, Chairman Engineering Faculties and Professor of Nuclear Engineering of Rensselaer Polytechnic Institute).

49. *See* N.Y. Times, Mar. 29, 1979, at 1, col.2.

50. Green, *supra* note 38, at 92; *see* Newman, *Control of Information Relating to Atomic Energy*, 56 YALE L.J. 769, 777-79 (1947) (calling the Restricted Data concept "sweepingly inclusive in scope").

51. *See Hearings on S. 3323 and H.R. 8862 To Amend The Atomic Energy Act of 1946 Before The Joint Committee On Atomic Energy — Part I*, 83d Cong., 2d Sess. 386-88 (1954) (hereinafter cited as *Hearings on S. 3323 and H.R. 8862*) (colloquy between Dr. William A. Higinbotham, Member, Executive Committee, Federation of American Scientists, and Representative Chester Holifield). As a way to limit the definition of Restricted Data, one witness suggested that data concerning "the use of special material in the production of power" be deleted from the definition. Restricted Data would then have been limited to weapons information and information concerning the production of plutonium and enriched uranium. *Id.* at 240 (statement of Theodore S. Kenyon, Chairman of the Atomic Energy Committee of the New York Patent Law Association). The suggestion was never adopted.

52. *Id.* at 407.

53. *See* notes 56-64 *infra* and accompanying text.

54. *See* note 75 *infra* and accompanying text.

55. *See* notes 76-77 *infra* and accompanying text.

56. 42 U.S.C. § 2161-2163 (1976). Functions formerly performed by the AEC are now performed by DOE and the NRC. *See* note 7 *supra*; 10 C.F.R. § 795 (1979).

57. 42 U.S.C. § 2161 (1976).

82-069 O—82——14 (Pt. 5) BLR

must permit and encourage the dissemination of scientific and technical information "so as to provide that free interchange of ideas and criticism which is essential to scientific and industrial progress and public understanding . . . ."[58] Indeed, the Act mandates a continuous administrative review of Restricted Data and any classification guides[59] so that determinations of which information may be properly declassified are kept current.[60]

Information constitutes Restricted Data by statutory definition alone. No affirmative classification by DOE or the NRC is contemplated or authorized. DOE and the NRC may prescribe regulations to protect Restricted Data[61] and they may establish degrees of sensitivity within the Restricted Data concept,[62] but they have no power to classify or reclassify information as Restricted Data.[63] They may de-

---

58. *Id.* § 2161(b).

59. *Id.* § 2162(b). DOE apparently has taken its declassification obligations seriously. Thousands of documents have been declassified and whole areas of research have been freed of security restraints. *See, e.g.,* [1970] AEC ANN. REP. 229 (1971). Despite such efforts, however, declassification will necessarily fall short of the statutory goal of making public all data that can be published "without undue risk to the common defense and security." 42 U.S.C. § 2162(a) (1976). Two basic reasons explain the inadequacy of the declassification program. First, the dynamics of administering any governmental secrecy program insure overclassification of information. Strong political and psychological forces impel classification officers to travel a safe path. The tendency, when in doubt, is to err on the side of secrecy. It is always easier to explain caution than it is to justify liberality, in part because the consequences of an error in favor of declassification seem far greater than an error in favor of secrecy. Once information is made public, it is forever compromised. If, however, it is mistakenly kept classified, it can be reviewed again. The strength of these tendencies is magnified under the Atomic Energy Act information control system because, unlike other government classification schemes, it is premised on Restricted Data being classified at birth. Declassification, not classification, takes an affirmative act. So, in addition to the usual leaning toward secrecy, atomic energy declassification must also overcome the force of inertia. Two features of the current declassification practice manifest the overclassification tendency. The first is known as derivative classification. Under derivative classification, persons who know the truth of a classified matter may not identify or indicate whether information in the public domain is in fact correct or accurate. If this is done, the identification or indication itself becomes classified. In addition, under derivative classification, the incorporation of any classified material directly or indirectly into an unclassified document renders the entire document classified. The second manifestation of the overclassification tendency is DOE's practice of declassifying an area of research only if the chance of developing classified information in that area is "essentially zero." *See* ATOMIC ENERGY COMMISSION, DIVISION OF CLASSIFICATION, GUIDE TO THE UNCLASSIFIED FIELDS OF RESEARCH 6 (1972).

The second inadequacy inherent in the atomic energy declassification program is the sheer volume of material that must be reviewed. Because the Restricted Data category is so broad, "continuous review" of such data, even if conducted in the utmost good faith, must always be cursory and out of date. For example, the only currently available document listing information that has been removed from the Restricted Data category is over six years old and acknowledged by DOE to be "obsolete." Letter from Murray L. Nash, Deputy Director, Office of Classification, Dept. of Energy, to author, March 15, 1979.

60. 42 U.S.C. § 2162(b) (1976).

61. *Id.* § 2201(i).

62. *Id.* § 2165(g).

63. *Id.* § 2162. This section is titled "Classification and declassification of Restricted Data — Periodic determination." The title is misleading; no power to classify is actually conferred. The original version of § 2162 did provide for classification authority but it was later amended. By a drafting oversight, the title was not similarly amended. *See* note 155 *infra*.

After the trial court had rendered its opinion in the *Progressive* case, *The Progressive* magazine discovered that the hydrogen bomb information the government successfully suppressed was actually contained in a document that had been available to the public at the government library in Los Alamos, for over four years. The govern-

classify information from the Restricted Data category only on a finding that it can be published without undue risk to the common defense and security. Unless such a finding is made, the information remains classified.[64]

This procedure is precisely the opposite of that which governs the classification of all other government documents. United States security classification practice is based principally on executive orders that apply, with a single exception,[65] only to information owned, produced or controlled by the government. The current order, Executive Order Number 12,065,[66] provides that government information may be withheld from public disclosure if there is an affirmative determination that it fits within one of the enumerated categories of classifiable information,[67] if disclosure would reasonably be expected to cause at least identifiable damage to the national security,[68] and if the identifiable harm is not outweighed by the public interest in disclosure.[69] Classified documents are automatically declassified after six years[70] or, at most, after twenty years. [71]

---

ment admitted that the publicly available information did indeed include such data, but it said that declassification, *i.e.*, publication, of the information was a "mistake." *See* note 276 *infra*. This turn of events appeared to raise the question whether DOE had the authority under the Atomic Energy Act, to reclassify information that it had previously declassified. The answer is clearly no. Under the Act, DOE has no authority to reclassify information. *See* S. REP. No. 1211, 79th Cong., 2d Sess. 23-24 (1946); *Hearings on S. 2236, supra* note 8, at 305; Green, *supra* note 38, at 92.

64. 42 U.S.C. § 2162(a) (1976).

65. The Invention Secrecy Act of 1951, 35 U.S.C. § 181-188 (1976); *see* note 71 *infra*.

66. Exec. Order No. 12,065, 3 C.F.R. § 190 (1978). The order defines classified information as information "that is owned by, produced for or by, or under the control of, the United States Government, and that has been determined pursuant to this Order or prior Orders to require protection against unauthorized disclosure. . . ." *Id.* § 6-102, 3 C.F.R. § 204. The order is the exclusive means of classifying government documents other than information governed by the Atomic Energy Act. *Id.* § 1-101, 3 C.F.R. § 191.

The order specifically prohibits classification of "basic scientific information not clearly related to the national security." *Id.* § 1-602, 3 C.F.R. § 194. Basic scientific information, however, is not defined. Moreover, the order specifically prohibits classification of privately developed information: information in which the government has no proprietary interest and that was developed without access to classified government data. An exception is made for information governed by the Invention Secrecy Act. *Id.* § 1-603, 3 C.F.R. § 194. Thus, under the order, the government may not impose secrecy on privately developed information even though that same information, in the hands of the government, would be classified. In short, no Official Secrets Act exists in the United States. For a general discussion of Exec. Order No. 12,065, see Fox & Weiss, *The FOIA National Security Exemption and the New Executive Order*, 37 FED. BAR. J. 1 (1978).

67. Exec. Order No. 12,065 § 1-301, 3 C.F.R. § 193 (1978).

68. *Id.* § 1-302, 3 C.F.R. § 193.

69. *Id.* § 1-303, 3 C.F.R. § 193.

70. *Id.* § 1-401, 3 C.F.R. § 193.

71. *Id.* § 1-402, 3 C.F.R. § 193. A classification of foreign government information, however, can last as long as thirty years.

Similar in operation to Exec. Order No. 12,065 is the Invention Secrecy Act, 35 U.S.C. §§ 181-188 (1976), the only statute that explicitly permits imposition of government secrecy over privately developed information. Under this Act, the government may impose a secrecy order over certain patents and patent applications whenever publication or disclosure of the invention might "be detrimental to the national security." *Id.* § 181. But under this Act, like Exec. Order No. 12,065 and unlike the Atomic

The Atomic Energy Act controls Restricted Data in two ways. First, espionage-like activities are prohibited. The espionage controls, sections 2274(a), 2275, and 2276, provide that communicating, disclosing, receiving, or tampering with Restricted Data with the intent to injure the United States or to secure an advantage to a foreign nation is punishable by a maximum term of life imprisonment.[72] Section 2274(b) punishes reckless or negligent disclosure — communication "with reason to believe such data will be utilized to injure the United States or to secure an advantage to any foreign nation".[73] Under this standard of culpability, prohibited communication could include activities such as public discussion about the efficacy of the government's atomic weapons program, publication of scientific discoveries in the atomic energy field, behavioral or other studies done on victims of atomic bombing or testing, or simply publication of any atomic energy material prior to ascertaining whether it included Restricted Data not yet officially declassified. Violation of section 2274(b) carries a maximum fine of $10,000, imprisonment for ten years, or both.[74]

Second, security controls limit access to Restricted Data to persons who have undergone a security investigation and who have obtained the proper security clearance.[75] Any present or former government employee, contractor, or licensee who knowingly discloses Restricted Data to persons unauthorized to receive it, that is, persons without clearance, is subject to a maximum fine of $2,500.[76] Furthermore, the DOE and the NRC may impose "such regulations or orders as [they] may deem necessary . . . to protect Restricted Data received by any person" under the terms of the Act.[77] Willful violation of such orders or regulations is punishable by a maximum fine of $5000, two years

---

Energy Act, a secrecy order issues only after an affirmative determination of possible detriment to national security. *Id.* Moreover, such orders may not last longer than one year unless a further finding of possible detriment to national security is made. *Id.*

72. 42 U.S.C. §§ 2274(a), 2275-2276 (1976).

73. *Id.* § 2274(b). The courts have not construed the meaning of this language in the Atomic Energy Act, but they have interpreted almost identical language in the Espionage Act, 18 U.S.C. § 793 (1976). "Advantage" has been broadly interpreted to mean help or assistance, and one may advantage a foreign nation without harming the United States. *See, e.g.*, Gorin v. United States, 312 U.S. 19, 29-30 (1941) (holding that the transfer of any national defense information helping a foreign nation was sufficient to establish a violation of the Act). Thus, communication may be proscribed if it in some sense "helps" another nation even though the communication does not harm the United States. *Id.* An article reviewing the espionage statutes at length concludes that the practical consequences of such a broad interpretation "is that if secret information relating to the national defense is transferred, reason to believe that advantage will result follows automatically. Other nations like to know what is going on and regard themselves as benefitted by whatever information they can obtain." Edgar & Schmidt, *The Espionage Statutes And Publication of Defense Information*, 73 COLUM. L. REV. 929, 987 (1973).

The "reason to believe" language has also been construed broadly. One has reason to believe communication will advantage a foreign nation if he is aware that an advantage will result. *See, e.g.*, Gorin v. United States, 312 U.S. at 27-28. Thus, one may want to reveal information to assist the United States, such as a new scientific discovery in the atomic energy field, but if he is aware that the revelation may also help other countries, he has satisfied the reason to believe standard.

74. 42 U.S.C. § 2274(b) (1976).

75. *Id.* § 2165(b). *See* 10 C.F.R. §§ 10.1-.37, 710.1-.38, 725.1-.31 (1979).

76. 42 U.S.C. § 2277 (1976).

77. *Id.* § 2201(i).

imprisonment, or both.[78] Violations of either the espionage controls or the security clearance controls may also be enjoined under section 2280.[79]

The information controls of the Atomic Energy Act raise important questions of statutory interpretation. The major question, long latent in the Act and finally raised in the *Progressive* case, is whether the Act applies to information developed by private citizens without government funding or access to classified government documents.[80] More specifically, does the "all data" terminology in the definition of Restricted Data mean all data, including privately developed data, or does it mean only all government data?

Furthermore, if the information controls of the Atomic Energy Act *do* apply to privately developed data, additional questions arise concerning the scope of those controls. For example, if a private citizen independently creates Restricted Data, is he subject only to the espionage controls of the Act, or is he also subject to the security clearance controls? More specifically, is he only prohibited from communication of the data with intent or reason to believe it will injure the United States or secure an advantage to a foreign nation, or must he obtain clearance to continue to possess his information and agree to communicate it only to others who also have clearance? Moreover, even if he is only prevented from engaging in espionage-like activities, does the prohibition against communication include a prohibition against publication?

These statutory questions should be discussed before addressing any of the constitutional issues raised by applying the Act to privately developed information because the consitutional questions need not be reached if the Act does not so apply. The statutory and constitutional issues are intertwined, however, and will be considered together because the very existence of serious constitutional objections triggers the application of particular canons of statutory construction. As every law student knows, if two interpretations of a statute are possible, one of which leads to a finding of unconstitutionality and one of which leads to a finding of constitutionality, a court must construe the legislation so as to uphold its validity.[81] Put another way, in the absence of a clear, express congressional statement, a court may not read a statute to authorize government action of

78. *Id.* § 2273.
79. *Id.* § 2280.
80. *The Progressive* raised only a narrow question of statutory interpretation in defending against the government's prior restraint action. It questioned only whether the Atomic Energy Act prohibits publication, as opposed to communication, of Restricted Data. 467 F. Supp. at 994. It did not ask the broader question, taken up here, whether the Act applies to privately developed information under any circumstances. *Id.*
81. *See, e.g.*, Lorillard v. Pons, 434 U.S. 575, 577 (1978); Johnson v. Robinson, 415 U.S. 361, 366-67 (1974).

doubtful constitutionality.[82] Before turning to the questions of statutory interpretation, however, it is helpful to examine how the government has actually tried to control privately developed information as Restricted Data.

III. Applications of Information Controls to Privately Developed Information

Government attempts to control privately developed information fall into two categories. First, the government has moved on at least two occasions to prevent the media from publishing information it believed fell into the Restricted Data category. Second, the government has from time to time imposed security clearance controls on such data in the hands of private enterprise.

In 1950, *Scientific American* magazine was about to publish, as part of its April issue, an article on the hydrogen bomb written by a noted atomic energy scientist and AEC consultant, Dr. Hans Bethe.[83] The editors of *Scientific American* did not submit the article to the AEC for security review because, in their view, "all the technical information in it was well known to physicists the world over and had been widely published."[84] The AEC nevertheless obtained a prepublication copy[85] and requested the deletion of certain portions of the article.[86] *Scientific American* complied, though reluctantly, and the offending portions of the article were removed.[87] At the AEC's request, and under its supervision, all copies of the original article together with the type and printed plates were destroyed.[88]

The facts of the *Progressive* case are similar.[89] In 1978, *The Progressive* commissioned a free-lance journalist to write a series of articles about secrecy in the United States nuclear weapons program. The

82. *See, e.g.*, Greene v. McElroy, 360 U.S. 474, 507 (1959); notes 191-92 *infra* and accompanying text.

83. Dr. Bethe's position in the *Scientific American* incident is somewhat ironic considering that he filed an affidavit on behalf of the government in the *Progressive* case. Indeed, his opinion that sizeable portions of *The Progressive* article should be classified carried great weight with the trial court. 467 F. Supp. at 993.

A major difference between the *Scientific American* and *The Progressive* articles is that the author of the *Scientific American* article, Dr. Bethe, served as a consultant to the AEC both before and after writing his article. As a consultant, he had a special relationship with the government and, presumably, access to secret government data. Consequently, his article can not accurately be described as privately developed.

In 1956, the AEC requested that its employees and consultants cease public discussion about thermonuclear reactions related to the then proposed hydrogen bomb project. The request stated that it applied to unclassified as well as classified information. The objective, as explained in telegrams to AEC managers, was "to avoid release of technical information which, even though itself unclassified, may be interpreted by virtue of the project connection of the speaker as reflecting the Commission's program with respect to thermonuclear weapons." *See* SCIENTIFIC AMER., May 1950, at 26. The AEC sent its request to all persons then or previously associated with the United States atomic energy program, which at that time included most of the atomic physicists in the country. *Id.*

84. *Id.*

85. *Id.* Dr. Bethe sent copies of his article to fellow scientists and colleagues, including a member of the AEC.

86. *Id.*

87. *Id.*

88. *Id.*

89. *But see* note 83 *supra.*

first article appeared in February 1979[90] and, though it contained some details of a hydrogen bomb production process, the government raised no objections to it.[91]

The second article, originally scheduled to appear in May 1979, contained further descriptions of hydrogen bomb manufacture including sketches showing how the bomb works. This time the government did object.[92] DOE informed the magazine that about twenty percent[93] of the article involved Restricted Data and offered to rewrite the piece to delete the "secret" information.[94] When *The Progressive* refused, the government invoked the Atomic Energy Act and obtained a preliminary injunction preventing publication.[95]

Magazines like *Scientific American* and *The Progressive* view privately developed atomic energy data as information within the public domain.[96] They claim the right to print as much of it as they consider newsworthy. The government, however, takes the position that under the Atomic Emergy Act, communication of such information may be enjoined or punished because it falls within the espionage provisions of the Atomic Energy Act.[97] The government claims that by publishing articles about the hydrogen bomb, the magazines are communicating Restricted Data with reason to believe it will harm the United States or secure an advantage to a foreign nation. And, in Catch-22 fashion, the magazines are said to have "reason to believe" because the government notified them that *it* has reason to believe that harm will result.[98]

The government's attempts to control privately developed atomic energy information in the hands of private enterprise other than the

---

90. THE PROGRESSIVE, Feb. 1979.

91. Presumably the government had no notice that the article was about to be published. It did have such notice with respect to the second article. *See* note 92 *infra*.

This problem of notice underscores one of the absurdities of applying information controls to privately developed information. The government can only prevent publication of information that it somehow learns will be published. Short of applying an unprecedented and unconstitutional screening of publications, the government can reach only those bits of information that the prospective publisher purposefully or inadvertently calls to its attention.

92. The managing editor of *The Progressive* sent draft copies of the hydrogen bomb article to several persons. One copy found its way into the hands of an MIT professor who, on his own initiative, sent it to DOE's Director of Classification. Learning of this, *The Progressive* decided to send DOE the sketches that were to accompany the article and ask whether the facts and sketches were accurate. Brief for the Defendant at 6, United States v. The Progressive, Inc., 467 F. Supp. 990 (W.D. Wis. 1979).

93. Prior to the issuance of the temporary restraining order, DOE refused to specify which portions of the article it found objectionable. It told *The Progressive* only that about 20% of the text, about six pages, and all of the captioned sketches contained Restricted Data. *Id.* at 5.

94. *Id.*

95. 467 F. Supp. at 1000.

96. Brief for the Defendant at 16-20, United States v. The Progressive, Inc., 467 F. Supp. 990 (W.D. Wis. 1979).

97. Brief for the United States at 3-11, United States v. The Progressive, Inc., 467 F. Supp. 990 (W.D. Wis. 1979).

98. *Id.* at 6-8.

press have followed a different, perhaps more invidious, pattern than its attempts to control media publication. The government apparently has seen no need to seek injunctions against private groups such as corporations to prevent them from working in the atomic energy field, nor has it instituted prosecutions for alleged espionage-like activities.[99] Rather, it has claimed the authority to impose security controls on private groups that independently generate information falling within the broad definition of Restricted Data.[100] Corporations, for example, may continue their work, but must first obtain security clearances for their personnel, agree to conform to all security regulations, and submit plans for safeguarding the data generated.

The administrative mechanism to implement this control is the Access Permit Program.[101] Under this program,[102] persons unassociated with government programs are given access to Restricted Data upon a showing of potential use or need for such data in their business, trade, or profession.[103] The government has administered the program not only as a means of permitting persons to gain entry to government information, but also as the basis for "permitting access" to information that someone develops and already posseses on his own[104] — a highly unusual notion of access.[105]

Just how does a company become involved in the net of security regulations? First, the government must learn in some way that a company is performing research in an area thought to include Restricted Data.[106] Consider the following, perhaps typical, hypothetical: Company X is performing research on advanced nuclear reactor design or engaging in some other activity arguably related to the production or use of atomic energy. The company either wants to check the reliability of its research findings with the government or is sufficiently informed about the Atomic Energy Act to wonder whether its research is patentable or even permissible. In either event, the company notifies DOE of its activities. DOE then informs the company that because the company's research findings fall within one of the categories considered to involve Restricted Data, it must obtain an access permit before it can continue its work or even remain in possession of its own information. Company X, believing there are no serious costs involved, follows the line of least resistance and complies. [107]

The costs of compliance, however, are substantial. The government immediately places limitations on the persons to whom the company

99. Research has disclosed no reported instance of any such proceeding.
100. *See* Green, *supra* note 38, at 105-06.
101. 10 C.F.R. § 725 (1979).
102. *See* Green, *supra* note 38, at 98-112.
103. 10 C.F.R. § 725.5(a) (1979).
104. *See Hearings on S.J. Res. 21, supra* note 8, at 268-70 (testimony of AEC General Counsel William Mitchell). *See also* Green, *supra* note 38, at 105-08.
105. *See* note 130 *infra*.
106. *See* note 91 *supra*; note 279 *infra*.
107. *See* Green, *supra* note 29, at 564-65.

may communicate Restricted information.[108] In addition, what the government giveth, the government can taketh away. Termination[109] or revocation[110] of the access permit is, in effect, a prohibition against the continued use or development of the information considered Restricted Data, and may mean a loss of whatever proprietary rights the company may have had in the data.[111]

The potential loss of the use of or control over one's own information is illustrated by the experience of four companies conducting private research on gas centrifuge enrichment technology in the 1960's.[112] The companies initially were granted access permits to carry on their research and later, after gas centrifuge research was removed from the Access Permit Program, were permitted to continue as "government contractors" under a "no-funds contract."[113] This arrangement proved mutually satisfactory until the government decided that "national security interests would be best served if privately sponsored work in the gas-centrifuge process for the separation of isotopes was discontinued."[114] Deprived of the right to use information developed by their own research, the companies suffered an obvious economic loss, with the result for one catastrophic because its entire business was development of gas centrifuge technology.[115]

Resistance to government imposition of atomic energy information controls on privately developed atomic energy information has been rare.[116] The *Progressive* case is the only instance of litigation brought against a noncomplying private party. The government may have been uneasy about litigating its authority in the face of resistance but, more likely, the government has found little need to go to court, given almost complete voluntary acceptance of information controls by private enterprise.[117] In any case, the government has never disavowed its authority to control privately developed atomic energy information.[118] Nevertheless, whether this authority was actually

108. *See* notes 126-28 *infra* and accompanying text. Complying with DOE regulations governing the safeguarding of Restricted Data, 10 C.F.R. § 795 (1979), also involves costs. *See* Green, *supra* note 29, at 562-64.
109. 10 C.F.R. § 795.38-.39 (1979).
110. *Id.*
111. *Id.*
112. Wash. Post, Mar. 22, 1967, at A 3, col. 3.
113. Wall St. J., Mar. 23, 1967, at 10, col.2.
114. *Id.*
115. *Id.*
116. *See Hearings on S. 2236, supra* note 8, at 281-82. The government has released no statistics to indicate how often it has imposed controls on privately developed atomic energy information. It appears, however, that the government has imposed these controls very infrequently. *Id.*
117. *See* Green, *supra* note 29, at 556, 564-65.
118. On the contrary, it has specifically claimed such authority. *See, e.g., Hearings on S.J. Res. 21, supra* note 8, at 268-70 (testimony of AEC General Counsel William Mitchell); *Hearings on S. 2236, supra* note 8, at 283.

granted by the Atomic Energy Act must still be determined.

IV. Statutory Interpretation

A. The Scope of the Restricted Data Definition

The central question of statutory interpretation is whether Congress intended the information controls of the Atomic Energy Act to apply to privately developed information. The government has long assumed that the controls so apply,[119] but the language and legislative history of the Act cast doubt on the inevitability of that conclusion.[120] Whether the act so applies depends upon whether Congress intended the concept of Restricted Data to embrace all atomic energy information or whether it intended such data to include only government owned or controlled atomic energy information.

1. The statutory language of the current law. The most direct support for an expansive interpretation comes from the all-encompassing definition of Restricted Data itself. Restricted Data is "all data" concerning atomic weapons and the use or production of special nuclear material.[121] The definition contains no qualification or exception concerning the source of the data — privately generated or government generated. Indeed, section 2162(e) of the United States Code implies that Restricted Data is not limited to data developed within the United States atomic energy program. Section 2162(e) provides a means of removing data "concerning the atomic energy programs of other nations" from the Restricted Data category and thus suggests that information generated outside federal programs is within the initial scope of the Restricted Data definition.[122] Similarly, section 2164, which sets out the terms of international cooperation in the atomic energy field, speaks of the "exchange" of Restricted Data with other nations.[123]

The patent sections of the Act offer further support for interpreting Restricted Data to include privately developed information. These sections presuppose that patent applications from private citizens can include Restricted Data.[124] For example, section 2223 provides that "[i]n the event that the [Atomic Energy] Commission communi-

119. *See* note 8 *supra*.

120. *See* notes 126-61 *infra* and accompanying text.

121. 42 U.S.C. § 2014(y) (1976).

122. *Id.* § 2162(e).

123. *Id.* § 2164(c). It would be incorrect, however, to make too much of the idea that Restricted Data can originate in foreign hands. Although the provisions dealing with Restricted Data of foreign origination presuppose that Restricted Data is not limited to information developed in the United States atomic energy program, they can be read as assuming that the Restricted Data of other nations is foreign-government-controlled and that this data comes to the United States under wraps, government to government, or government to spy to government, just like any other secret foreign government information.

124. *Id.* §§ 2181-2190 (1976). Significantly, these sections do not speak of patents in terms of Restricted Data. Rather, they speak of inventions or discoveries "useful in the production or utilization of special nuclear material or atomic energy." *Id.* § 2181(c). Of course, Restricted Data is "all data" related to such matters, but Congress's failure to use the Restricted Data terminology may indicate that it understood that information

cates to any nation any Restricted Data based on any patent application not belonging to the United States, just compensation shall be paid. . . ."[125]

Despite these indications that the definition of Restricted Data includes privately developed information, other provisions of the Act fail to support an expansive view of Restricted Data. These provisions presume that such data is strictly government originated and controlled. To illustrate, the Act sets out the terms and conditions under which government employees, private enterprises, and private persons may obtain access or admittance to Restricted Data.[126] The Act requires government contractors and licensees to agree not to permit unauthorized individuals to have access to Restricted Data.[127] The act also prohibits present or former government employees and agents from disclosing Restricted Data to persons not entitled to receive it.[128] These and similar provisions[129] make sense only on the assumption that the government is the sole source and repository of Restricted Data.[130]

2. Legislative history — The 1946 Act. The concept of Restricted Data originated in the Atomic Energy Act of 1946 and has remained essentially unchanged since then.[131] The legislative history of the 1946 Act offers indirect but ultimately inconclusive support for the view that atomic energy information controls were meant to apply to privately developed information.

The Atomic Energy Act of 1946 began as S. 1717, drafted by Senator Brien McMahon, Chairman of the newly created Senate Special Committee on Atomic Energy.[132] A major task in drafting S. 1717 was

---

"useful in the production or utilization of special nuclear material or atomic energy" could not be Restricted Data while in private hands.

125. *Id.* § 2223. Again, however, this language may be read consistently with the view that Restricted Data is only government data. First, a patent may not belong to the United States and yet be based on research performed by the inventor while serving as a government contractor or licensee. *Id.* § 2182. Second, the patent provisions provide a means by which the government may, upon payment of just compensation, appropriate patents related to atomic energy inventions. *Id.* § 2181(b). Once such an appropriation is made under the special procedures of the patents section, the data involved may become government data, and hence Restricted Data.

126. *Id.* § 2163 (1976).

127. *Id.* § 2165(a).

128. *Id.* § 2277.

129. *See, e.g., id.* §§ 2165(b), 2201(i).

130. It might be argued that the word "access" was used to mean "legal access." A private citizen, for example, can generate information on his own and thus by definition have access to it, but, unless and until he obtains the government's permission to maintain possession, he does not have the requisite "legal access." Not only is there no evidence that Congress intended to use the word access in this unusual way but, if the word is so used, the provision requiring government contractors to agree not to permit unauthorized individuals to have access to Restricted Data would become unintelligible. Government contractors would be agreeing not to give unauthorized persons "legal access" — something they are not empowered to give under any circumstances.

131. *See* notes 43, 51-52 *supra.*

132. S.1717, 79th Cong., 2d Sess. §§ 1-17 (1946). McMahon's bill was not, however, the

to write information controls that would reconcile security needs with scientific freedom.[133] Initially, S. 1717 distinguished between "basic scientific information", defined as theoretical knowledge of physics, chemistry, biology, and therapy in all fields of atomic energy research, and "related technical information", indirectly defined as the "processes or techniques" incorporating theoretical atomic energy information.[134] Under section 9 of S. 1717, all basic scientific information was completely in the public domain, but all related technical information was controlled by the Atomic Energy Commission.[135] Moreover, security protections for these technical data were tied to the Espionage Act.[136]

The Special Committee on Atomic Energy held extensive hearings on S. 1717.[137] References to the desirability of keeping certain privately generated atomic energy information under government control were general and not tied to specific provisions of S. 1717.[138] The chief concern expressed by both committee members and witnesses was the need to protect secrets about atomic bomb manufacture, which only the government would possess.[139] Witnesses also noted the conflicting need to disseminate atomic energy information freely to foster scientific progress.[140]

Following the hearings, the Special Committee substantially revised S. 1717, including its information section.[141] The new informa-

---

first comprehensive atomic energy legislation proposed in Congress. The first was a bill drafted by the War Department and introduced in the House as H.R. 4280 on October 3, 1945. Known as the May-Johnson bill, it would have created a nine-member Atomic Energy Commission with sweeping authority to control all aspects of atomic energy production, research, and development. *See* H.R. 4280, 79th Cong., 1st Sess. (1945). The Secretary of War and the sponsors of the legislation hoped to speed the bill through Congress but stiff opposition from scientists plus a jurisdictional wrangle in the Senate stalled and ultimately killed the bill after only two days of hearings before the House Committee on Military Affairs. *See* Miller, *supra* note 24, at 801-05. *See generally Hearings Before the House Comm. on Military Affairs on H.R. 4280,* 79th Cong., 1st Sess. (1945). Scientists and others testifying on H.R. 4280 made clear that the "secret" of the atomic bomb was basic scientific information that was open to anyone else to discover in time and that the real "secret" — that an atomic bomb could be built — was already known. The secrets remaining to be protected were secrets of know-how and information related to the direction of the United States's atomic energy research. *See, e.g., id.* at 12-13, 80, 117-18.

133. 92 CONG. REC. 6096 (1946).

134. S. 1717, 79th Cong., 2d Sess. § 9 (1946). Atomic scientists endorsed this approach. *See* HEWLETT & ANDERSON, *supra* note 22, at 483.

135. S. 1717, 79th Cong., 2d Sess. § 9 (1946). S. 1717 directed the Commission to establish a Board of Atomic Information that would be responsible for regulating the dissemination of related technical information. *Id.*

136. *Id.* §§ 3, 9.

137. *Hearings Before the Special Senate Comm. on Atomic Energy on S. 1717,* 79th Cong., 2d Sess. (1946) (hereinafter cited as *Hearings on S. 1717*).

138. *See, e.g., id.* at 404-10, 492. For example, Major General L. R. Groves, head of the wartime atomic bomb project, stated, "I don't believe that if we make some startling discovery in a college laboratory that that should necessarily be published if it is going to upset our national defense. . . ." *Id.* at 492.

139. *See, e.g., id.* at 404, 407.

140. *See, e.g., id.* at 122-23, 404, 407.

141. *See* HEWLETT & ANDERSON, *supra* note 22, at 512. The members of the Special Senate Committee apparently viewed the information controls with disfavor. They seemed to think that more comprehensive controls were needed and they doubted whether the Espionage Act could be made applicable to the protection of atomic energy information during peacetime. *Id.* Ironically, while the Committee was considering the McMahon version of S. 1717, Canadian authorities announced the arrest of 22

tion section, renumbered section 10, scrapped the distinction between basic scientific information and related technical information.[142] A new term, Restricted Data, was coined and defined to include "all data concerning the manufacture or utilization of atomic weapons, the production of fissionable material, or the use of fissionable material in the production of power, but shall not include any data which the Commission from time to time determines may be published without adversely affecting the common defense and security."[143] All references to the Espionage laws were dropped and special criminal provisions, paralleling those of the Espionage Act, were added and made applicable to the misuse of Restricted Data.[144]

Senate debate on the revised S. 1717 was brief.[145] The sense of the debate, like the testimony of witnesses before the Special Committee, was that all vital atomic energy information concerned weapons or was weapons-related and that all such information was government owned and controlled. The debate did not mention the need to preserve secrecy over privately generated atomic energy information. The House debates on S. 1717 were similarly silent.[146] The implication, therefore, is that Congress did not consider privately developed information to be in need of the same protections as government owned data.

The only direct and unequivocal support for construing the atomic energy information controls to apply to privately developed information is found not in the language or legislative history of the 1946 Act, but in a book written by James R. Newman, Counsel to the Special Committee, and Byron S. Miller, staff member of the committee and a

---

persons in connection with passing very sensitive United States atomic energy information to the Soviet Union. No American citizen was involved but the event created a stir in the press and presumably hardened the Committee's attitude toward information controls. *Id.*

142. S. 1717, 79th Cong., 2d Sess. § 10(b)(1) (1946), *reprinted in* [1946] U.S. CODE CONG. SERV. 722, 732-34.

143. *Id.*

144. *Id.*

145. 92 CONG. REC. 6096-98 (1946).

146. *Id.* at 9249-75. Like the Senate debates, the House debates reflect congressional concern with preserving the secret of the atomic bomb lest that secret fall out of government hands. The legislative reports on S. 1717 offer no guide to or hint about the proper scope of the concept of Restricted Data. S. REP. NO. 1211, 79th Cong., 2d Sess., *reprinted in* [1946] U.S. CODE CONG. SERV. 1327. In the House, S. 1717 was referred to the Committee on Military Affairs. The Committee held no hearings and reported the bill favorably after adopting amendments to insure military participation on the Atomic Energy Commission. The Committee report on S. 1717 is a straight-forward, section-by-section description of the legislation, and is largely irrelevant to the present discussion. *See* H.R. REP. NO. 2478, 79th Cong., 2d Sess. (1946). On the floor, the House amended S. 1717 in several ways. With respect to information controls, it added a provision requiring FBI investigation and clearance of all AEC Commissioners, employees, licensees, and contractors, and it increased the penalties for espionage activities from a maximum of 20 years imprisonment to death. 92 CONG. REC. 9482 (1946). The Senate agreed to these amendments, refused others, and the Atomic Energy Act finally passed both houses on August 1, 1946. *Id.* at 10329, 10411 (1946).

draftsman of S. 1717.[147] They state:

> "Restricted data," as the Act defines the term, goes far beyond the classification of atomic weapons and includes data "relating to the production of fissionable material, or the use of fissionable material in the production of power." These categories cover a very large area of nuclear science and embrace much that is of general importance to fundamental as well as to applied research. It does not matter whether these data are discovered or compiled in a government laboratory or in connection with the private research of an individual scientist; the interdict covers them in either case.[148]

The views of Newman and Miller must be given weight, but precisely how much is uncertain. No doubt, Senator McMahon and other members of the Special Committee knew of Newman and Miller's views. There is no evidence, however, that the Committee shared their interpretation, and, more importantly, there is no evidence that Congress as a whole similarly understood or interpreted the provisions of section 10.

3. Legislative history — The 1954 Act. After 1946, rapid advances were made in the development of peaceful and military uses of atomic energy both in the United States and worldwide. Congress kept abreast of these developments through the work of its Joint Committee on Atomic Energy, a special committee created by the 1946 Act.[149] In 1954, the Committee began drafting major amendments to the 1946 Act. Their work was embodied in two companion bills introduced as S. 3323 and H.R. 8862.[150]

---

147. J. NEWMAN & B. MILLER, THE CONTROL OF ATOMIC ENERGY (1948).

148. *Id.* at 15; *see id.* at 224-25.

149. *See Hearings Before the Joint Comm. on Atomic Energy on Investigation into U.S. Atomic Energy Project—Part III*, 81st Cong., 1st Sess. 104-39 (1949). For example, in 1949 the Joint Committee held extensive hearings on all aspects of the United States atomic energy program. The concept of Restricted Data was discussed at some length but the focus was on emergency clearance procedures used by the AEC that enabled persons to work for the Commission temporarily without clearance. The question was whether the procedures were being employed too loosely. Significantly, the discussion was exclusively in the context of access to Restricted Data as controlled and possessed by the government. *See Hearings before the Joint Committee on Atomic Energy on Investigation into U.S. Atomic Energy Project—Part III,* 81st Cong., 1st Sess., at 104-39 (1949).

150. *See* H.R. 8862, 83d Cong., 2d Sess. (1954); S. 3323, 83d Cong., 2d Sess. (1954) These bills originated as a Joint Committee print entitled 'A Proposed Act to Amend the Atomic Energy Act of 1946.' JOINT COMM. ON ATOMIC ENERGY, 83D CONG., 2D SESS. (Comm. Print 1954) (hereinafter referred to as Comm. Print). H.R. 8862 was introduced in the House by Rep. Cole on April 15, 1954 and S. 3323 was introduced in the Senate by Sen. Hickenlooper on April 14, 1954. H.R. 8862, 83d Cong., 2d Sess. (1954); S. 3323, 83d Cong., 2d Sess. (1954). The bills proposed several changes with respect to Restricted Data and the controls on atomic energy information. First, the definition of Restricted Data was changed slightly. Comm. Print § 11(q). It was expanded to include all data concerning the "design" of atomic weapons as well as the manufacture and utilization of such weapons, and fissionable material was renamed special material. *Id.* § 11(s). A second and more fundamental change was the addition of a provision for automatic declassification of Restricted Data after three years "unless there is a specific finding made . . . that the common defense and security require that the Restricted Data retain its classification for an additional . . . three years." *Id.* § 145(c). This provision was ultimately scrapped. *See* note 155 *infra*. Third, the AEC was empowered to tailor its security clearance procedures in accordance with the degree of sensitivity of Restricted Data "to which access will be permitted." Comm. Print § 142(f); *see* notes 61-63 *supra* and accompanying text. This change reflected the fact that private enterprise was about to be admitted to the atomic energy field. Fourth, new criminal provisions

The Joint Committee held two sets of hearings on the proposed bills.[151] The testimony indirectly reflected a certain measure of confusion among committee members and witnesses about whether and to what extent information controls over Restricted Data encompassed privately generated information. For example, by written statement, E. Blythe Stason, Dean of the University of Michigan Law School, posed the following question to the committee: "Does 'Restricted Data' include data developed prior to the time it is reported to the Commission under section 103 and classified then as restricted?"[152] He continued, "This is important especially since the penalty provisions of section 223 [new criminal penalties] are severe. If private operators are to proceed in such cases at their peril it should be made clear in the act."[153] Unfortunately, his question was either overlooked or simply ignored. The committee also heard from Jerome Luntz, editor of *Nucleonics* magazine, and Oscar Reubhausen, Chairman of a Special Committee of the New York City Bar Association. Both witnesses seemed to think that Restricted Data could be created by private persons but, again, their testimony exhibited a considerable degree of uncertainty about the issue.[154]

---

were added making it a crime for current or former government employees to communicate Restricted Data to persons not entitled to receive it and making it a crime to receive Restricted Data from such a person. Comm. Print §§ 223(d), (e). Finally, a new section on international cooperation was proposed. Under certain circumstances the United States could exchange Restricted Data with other nations, but, in no event, could the Restricted Data involve weapons information. *Id.* § 144(a).

151. *Hearings on S. 3323 and H.R. 8862*, note 51 supra.

152. *Id.* at 63.

153. *Id.*

154. *Hearings on S. 3323 and H.R. 8862 supra* note 51, at 51-53. Mr. Luntz, for example, seemed to think that publishers could publish all information revealed to them by the AEC through proper channels and any other information they discovered, provided they were not put on notice, constructive or otherwise, that it was classified. He believed that the new criminal provisions, which made it a crime to receive Restricted Data from present or former government employees, might change the rule as he understood it. He testified, in part, as follows:

> Mr. Luntz: As far as publishers are concerned, we on Nucleonics have never had any problem regarding the classification of material we planned to publish. Articles that come to us from AEC labs are cleared through routine channels. Anything that we write on our own is publishable because we have no clearance and are not obligated nor permitted to know what is classified.
>
> Chairman Cole: What do you mean, you are not permitted to know what was classified? If I wanted to tell you something that was classified, you wouldn't let me tell you?
>
> . . . .
>
> Mr. Luntz: We are legally not permitted to be told it by someone who has the information.
>
> . . . .
>
> A more specific example of something that might happen to the press is this: Suppose we asked the AEC about the possibility of our getting an article on something like the fabrication of fuel elements for reactors. And suppose that we were advised that this is a classified area . . . . Then, suppose that shortly thereafter we received an unsolicited article from a foreign nation on this very subject.

Both houses passed the bills, redesignated H.R. 9757 and S. 3690, after extensive debate amd numerous amendments.[155] Relative to

---

. . . .

Because we might have reason to believe that the article contained restricted data, my question would then be: What is our fate if we were to publish this article?

I believe that the primary accomplishment of sections 223d and 223e would be to create an atmosphere of intimidation and harassment. The relatively low fine of $2,500 implies to me that much more than this may not have been intended.

Coverage of the atomic energy field by the nonspecialist technical and non-technical press has to date been inadequate, in my opinion — inadequate from the point of view of providing the technical and nontechnical public with information they need for their guidance, and, what may be more important, information they need to provide intelligent and constructive criticism of the Government program.

One of the reasons for the poor coverage of this field by the press, and I have observed this repeatedly, is the prevalent feeling that this whole thing is too secret and the effort to develop a story just isn't worth it. One effect of the new amendments might be to reduce what little coverage there is.

Id.

Mr. Ruebhausen also was uncertain about the effect of the new criminal provisions and the following testimony illustrates that he was not alone in his uncertainty:

Rep. Durham: Do you think it would be possible, or would it be reasonable, for a physicist who has of course full knowledge of practically all of these developments, who has never had contact with the AEC, who has never seen a classified document, to write an article in a newspaper which could be construed as being classified material? It looks to me like it is possible. And that is the point that worries me so as to this "has reason to believe." I do not know how you are going to get at it, because I think it is one of the most difficult problems we face in the whole writing of the act. I mean by that that if we write it to the point where we are going to let people freely receive some type of information, I think we will not reach the goal which we are trying to accomplish here.

Mr. Ruebhausen: I am very troubled by it, too, sir. . . . It is the complete absence of any exception for the wholly innocent communication which bothers me. Maybe we have no other alternative than to penalize the innocent with the guilty. But before we do it, it is a very drastic step, and I know the committee will search for ways to soften it.

. . . .

Rep. Holifield: Mr. Ruebhausen, I am also concerned with this particular subject of declassification of restricted data, particularly in view of the all-inclusive meaning of the word "design" in the definitions section, particularly using the work "design" in the restricted data section. It seems to me that it covers almost the complete field of research and development as well as application. And then placing the punitive section with relation to these people — it seems to me that it does present us a real problem. I believe with Congressman Hinshaw that there are a great many articles that are printed today in different magazines which, in effect, too, reveal either speculatively or from some source that I know not of, restricted data.

Id. at 405-06.

155. At the close of Part I of the hearings, the Joint Committee met in executive session and amended the information control sections of the Committee Print in two significant ways. First, it deleted the automatic declassification provision and, in its place, empowered the AEC to classify as well as declassify information as Restricted Data. *See Hearings on S. 3323 and H.R. 8862, supra* note 51, at 713. Under the new language, Restricted Data would no longer be classified automatically by statutory definition. *See* 42 U.S.C. § 2162 (1976). Rather, the AEC would have to make an affirmative classification decision. *Id.* Second, the Committee tightened the new criminal provisions proscribing the communication of Restricted Data by present or former government employees to persons unauthorized to receive it. *See Hearings on S. 3323 and H.R. 8862, supra* note 51, at 708. The new language added that, as an element of the crime, the person communicating the Restricted Data must know or have reason to know the information was Restricted Data and that the person receiving it was unauthorized. 42 U.S.C. § 2277 (1976). After the second round of hearings, the Committee made only one major change relating to Restricted Data. The Committee voted to retain the existing language of the 1946 Act which classified Restricted Data by statutory definition alone. In other words, it eliminated the provision whereby the AEC was

the total amount of discussion on the proposed bills, the debate concerning Restricted Data was quite limited[156] and centered almost entirely on three points: concern over the United States giving Restricted Data to other nations under the new provisions for international cooperation,[157] support for tightening the criminal provisions to prevent government employees from giving Restricted Data to persons not authorized to receive it,[158] and support for permitting the Atomic Energy Commission to tailor its clearance procedures and harmonize its classification responsibilities with the classification regime of the Department of Defense.[159] There was no debate about application of Restricted Data controls to privately developed information and, again, all references to Restricted data implicitly assumed that all such information was government controlled, developed, or owned.[160]

The central conclusion to be drawn from the statutory materials of the 1946 and 1954 Acts is that, if Congress intended to control privately developed atomic energy information, it did so in a highly ambiguous, equivocal, and uncertain way. The legislative history does offer some support for the view that Congress did intend this result, but such a broad interpretation is hard to square with the almost complete silence on the matter in the legislative hearings, reports, and debates. Moreover, assuming that Congress contemplated some means of controlling highly sensitive or important new discoveries in the atomic energy field, that control was arguably provided for in both the 1946 and 1954 Acts in provisions requiring certain reporting of new discoveries and in provisions limiting patents in specific areas.[161] Finally and most significantly, the language of the current law,

---

charged with classification and declassification. Apparently, the Committee was persuaded by the testimony of Assistant Attorney General J. Lee Rankin, who testified that a Commission obligation affirmatively to classify information would jeopardize prosecutions of espionage violations of the Act. *See Hearings on S. 3323 and H.R. 8862, supra* note 51, at 718-20. He claimed that the new provision would require the prosecution to show that the allegedly compromised information was properly classified as Restricted Data. *Id.* at 718. Such proof, he said, might force the government to introduce into evidence its Classification Guides — some of which are themselves classified. *Id.* at 718.

The Senate and House Reports on S. 3323 and H.R. 9757 are of little help in deciding whether Congress intended the information controls to extend to privately developed information. They support only the implication that Congress was assuming that Restricted Data was exclusively government owned or controlled. *See* S. REP. No. 1699, 83d Cong., 2d Sess. 6-9, 21-22, 23-24 (1954); H.R. REP. No. 2181, 83d Cong., 2d Sess. 6-9, 21-22, 23-24 (1954). Finally, the Conference Reports are essentially uninformative on the question. *See* CONF. REP. No. 2639, 83d Cong., 2d Sess. 24-27 (1954); CONF. REP. No. 2666, 83d Cong., 2d Sess. 24-27 (1954).

156. *See, e.g.*, 100 CONG. REC. 10564-66, 11580, 11655-60, 11671-72, 11719-20 (1954).

157. *See,e.g., id.* at 10564-68.

158. *Id.* at 11671, 11750-51.

159. *Id.* at 10565.

160. *Id.* at 10564-66, 11580, 11655-60, 11671-72, 11719-20.

161. Atomic Energy Act of 1954, §§ 151-160 (current version at 42 U.S.C. §§ 2181-2190 (1976)); Atomic Energy Act of 1946, § 11 (current version at 42 U.S.C. §§ 2181-2296 (1976)).

practically unchanged since 1954, reflects the view that Congress believed Restricted Data was only government data.[162]

B. Security Clearance Controls Over Privately Developed Information

Assuming that the Atomic Energy Act does reach privately developed atomic energy information, a second question of statutory interpretation arises: is this information subject only to the law's espionage controls or is it also subject to the law's security controls? The answer carries significant practical consequences for companies or other private groups such as universities working in the atomic energy field.[163] If a company generating Restricted Data is subject only to the prohibition against engaging in espionage-like activities, then it is only prevented from communicating its research information with intent to injure or with reason to believe such communication will injure the United States or secure an advantage to a foreign nation.[164] Because the espionage prohibitions require proof of criminal intent, they are not likely to create a substantial threat of criminal prosecution for communicating Restricted Data in the ordinary and customary context of a domestic business.[165] If, however, the company is also legally subject to security controls, then the company must be admitted to the Access Permit Program before it may continue its work.[166] In other words, it must have its personnel undergo security investigations and obtain security clearances, it must agree to all rules and regulations of DOE or the NRC governing the safeguarding of Restricted Data, and it risks the loss of its information if the government revokes or terminates the Access Permit.

The question whether security controls apply to privately developed information turns on the more specific question whether Congress intended to confer such powers on DOE, the NRC, or the former AEC. Under the 1946 Act, the AEC had no authority to control restricted data in the hands of persons unassociated with the government. The 1946 Act provided only that before the AEC entered into any contract, granted any license, or hired any person, the prospective contractor, licensee, or employee had to undergo an investigation by the FBI and be found trustworthy by the AEC.[167]

In 1953, the Act was amended to permit the AEC to promulgate

---

162. *See* notes 127-30 *supra* and accompanying text.

163. *See* notes 101-16 *supra* and accompanying text.

164. *See* 18 U.S.C. § 793 (1976). Note, however, that the similar but different provisions of the Espionage Act also may apply.

165. A business could substantially reduce, if not eliminate, such a threat by adopting internal procedures to limit access to certain employees and to specify how such information should be handled. First, access could be limited to persons with a proven record of loyalty and reliability and with a business need to know the information. Second, all documents containing Restricted Data could be stamped with a legend notifying employees that wrongful communication could result in criminal prosecution. Finally, information could be stored in a manner to insure its integrity.

166. *See* notes 101-05 *supra* and accompanying text.

167. S. 1717, 79th Cong., 2d Sess. § 10(b)(5)(B) (1946). These requirements originated as House floor amendments and consequently received little study or attention. *See* HEWLETT & ANDERSON, *supra* note 22, at 527-30.

such rules and regulations "as may be necessary to carry out the purposes of the Act."[168] In 1967, the AEC relied on this provision as statutory authority for proposed regulations aimed at controlling "private Restricted Data."[169] Nothing in the legislative history of the amendment, however, supports the AEC's view that it was a grant of authority to control this kind of information. To the contrary, the legislative history reveals that the amendment was designed to confer on the AEC only those powers "ordinarily granted to administrative agencies"[170] and specifically that it was not meant to "enlarge any powers of the Atomic Energy Commission to issue rules and regulations that would subject violators thereof to criminal punishment."[171]

In the Atomic Energy Act of 1954, one new provision offered some superficial support for the view that the AEC was granted authority to control privately developed information. The new provision read:

> Except as authorized by the Commission or the General Manager upon a determination . . . that such action is clearly consistent with the national interest, no individual shall be employed by the Commission *nor shall the Commission permit any individual to have access to Restricted Data until . . . the Commission shall have determined that permitting such person to have access to Restricted Data will not endanger the common defense and security.*[172]

This language could be interpreted to mean that the AEC's authority to control the dissemination of Restricted Data extended beyond its own employees, licensees, and contractors to include "any individual." On close analysis, however, this provision proves inadequate to support such a broad reading of the AEC's authority. The better view is that the new provision was intended to limit only persons who may have access to *government* controlled Restricted Data. Almost every reference to Restricted Data in the legislative history of the 1954 Act implicitly reflects the view that the government's atomic energy program was the source and repository of Restricted Data.[173] Thus, Congress contemplated that Restricted Data was something to be obtained from and given by the AEC. It was not something the AEC was to control when it originated in the private sector.

Two other provisions, new in the 1954 Act, support the view that the AEC's regulatory authority over Restricted Data is limited to controlling such information in the hands of its employees, licensees, and contractors. First, section 161(i) authorized the AEC to prescribe

168. Act of July 31, 1953, ch. 283, § 7 (amending § 12(a)(10)), 67 Stat. 240 (current version at 42 U.S.C. § 2201(p) (1976)).
169. 32 Fed. Reg. 6702, 6706, 6710, 20868 (1967).
170. S. REP. No. 603, 83d Cong., 1st Sess. 4 (1953).
171. *Id.*
172. Atomic Energy Act of 1954, § 145(b) (current version at 42 U.S.C. § 2165(b) (1976)) (emphasis added). Section 145(b) of the 1954 Act amended former section 10(b)(3)(ii) of the 1946 Act, which directed the AEC to require security clearance and investigation of all AEC employees. *See id.*
173. *See* notes 156-60 *supra* and accompanying text.

such regulations and orders as it may deem necessary ". . . to protect Restricted Data *received* by any person in connection with any activity authorized pursuant to this Act. . . ."[174] The clear import of this language is that such orders or regulations will be applicable only to persons engaged in some activity authorized under the Act.[175] Therefore, it would not apply to a private person (who is not a contractor or a licensee, or one with whom AEC had entered into an arrangement) who is engaged in an activity that does not require AEC authorization. Moreover, an order or regulation would not apply only to Restricted Data that is internally generated rather than "received" from an external source; moreover, it would not apply to Restricted Data that is "received" other than in connection with an authorized activity.

The second and most important provision of the 1954 Act relevant to construing the scope of AEC's regulatory authority is section 2166(b), which provides that "The Commission shall have no power to control or restrict the dissemination of information other than as granted by this or any other law."[176]

Although neutral on its face, this provision reveals the sense of Congress that the AEC's authority was to be narrowly construed and specifically limited to those powers expressly granted.[177] A power not expressly granted was the power to control privately developed information.

Viewing the statutory provisions as a whole and in light of their legislative hsitory, the AEC had (and DOE and the NRC now have) no statutory authority to control the use, handling, or dissemination of Restricted Data generated by persons unassociated with the government. If this information is governed by the Atomic Energy Act at all, it is governed only by the law's espionage controls.

C. Espionage Controls Over Privately Developed Information — Communication As Publication

Assuming, again, that the information controls of the Atomic Energy Act apply to privately developed information, the final question of statutory interpretation is whether the espionage prohibitions against communicating Restricted Data include prohibitions against publishing it. In *United States v. The Progressive, Inc.*, *The Progressive* magazine argued unsuccessfully that even if its hydrogen bomb article contained Restricted Data, the Atomic Energy Act did not pre-

174. Atomic Energy Act of 1954, § 161(i) (current version at 42 U.S.C. § 2201(i) (1976)) (emphasis added).

175. *See* Reynolds v. United States, 286 F.2d 433 (9th Cir. 1960). In *Reynolds*, the Ninth Circuit concluded that § 161(i) applied only to Commission licensees. *Id.* at 438.

176. Atomic Energy Act of 1954, § 146(b) (current version at 42 U.S.C. § 2166(b) (1976)).

177. The provision was so interpreted by AEC officials. The AEC opposed the inclusion of § 146(b) in the 1954 Act, arguing that it "seems intended to deprive the Commission of implied or inherent authority" and "might have most undesirable consequences, particularly with respect to security matters." *Hearings on S. 3323 and H.R. 8862, supra* note 51, at 605. In spite of such testimony the Joint Committee rejected the AEC's plea to eliminate § 146(b).

vent the "publication" of this information because it proscribed only the "communication" of Restricted Data.[178] In *The Progressive*'s view, publication and communication are not synonymous; if Congress intended to prohibit publication, it would have said so specifically.[179]

The genesis of the *Progressive* argument was dicta in the opinions of several justices in *New York Times Co. v. United States*.[180] There, in three separate opinions, five justices agreed that the Espionage Act did not prevent the publication of the Pentagon Papers because it provided:

> [w]hoever having unauthorized possession of . . . information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates . . . the same to any person not entitled to receive it . . . [s]hall be fined . . . or imprisoned.[181]

The Act did not expressly provide that publication was similarly proscribed.[182]

Although the criminal provisions of the Atomic Energy Act are modeled after the criminal provisions of the Espionage Act, there are significant differences in the proper construction of the two statutes. The Atomic Energy Act, like the Espionage Act, punishes certain "communication" of information.[183] Unlike the Atomic Energy Act, however, the Espionage Act contains other sections that do proscribe publication of information.[184] Moreover, the legislative history of the Espionage Act reveals that Congress considered, but rejected, a broader version of section 793 that would have authorized media censorship.[185]

Standing alone, the language of the Atomic Energy Act gives no hint whether Congress meant the word communicate to include the word publish. Under a plain meaning rule, however, it is difficult to see why publication would not be considered a form of communication. Commonly understood, publication is a subset of communication, one means of accomplishing it.[186] Moreover, if harm may result from disclosing atomic energy information, it will result as surely from publication as from any other form of communication. Finally,

178. Brief for Defendant at 26, United States v. The Progressive, Inc. 467 F. Supp. 990 (W.D. Wis. 1979).
179. *Id.*
180. 403 U.S. 713 (1971).
181. *Id.* at 720 (quoting 18 U.S.C. § 793(e) (1976)).
182. 403 U.S. at 720-22 (Douglas, J., concurring); *id.* at 733-34 (White, J., concurring); *id.* at 746 (Marshall, J., concurring).
183. *Compare* 42 U.S.C. § 2274(b) (1976) *with* 18 U.S.C. § 793(e) (1976).
184. 18 U.S.C. §§ 794(b), 797-798. *See* Edgar & Schmidt, *supra* note 73, at 944, 1064, 1069.
185. *See* Edgar & Schmidt, *supra* note 73, at 1019.
186. *See* WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 1836 (1963). Publication has been defined as "communication (as of news information) to the public."

the legislative history shows that both witnesses and Congressmen used the terms interchangeably[187] — though no one apparently anticipated that the prohibitions of section 2274 would be read together with the injunction section to permit prior restraints.

The legislative hearings on the 1946 Act indicate that, to the extent that Congress may have considered the information controls applicable to privately developed information, it had the work of scientists in mind.[188] Congress was well aware that scientists routinely publish their results. In this sense, Congress may have used communication as a generic term encompassing this form of publication.

The legislative hearings on the 1954 Act offer more direct evidence. The testimony of the editor of *Nucleonics* magazine, together with correspondence from The American Society of Newspaper Editors, The Associated Business Publications, and others, shows that the media read communication to include publication.[189] In 1954, media representatives expressed concern that the new provisions punishing the communication of Restricted Data received from present or former government employees would impose a burdensome obligation on the media by requiring prepublication determinations whether information to be published was restricted.[190]

In sum, all available statutory evidence, though admittedly meager, leads to the conclusion that prohibitions against communicating Restricted Data include, and were meant to include, prohibitions against publication of that data. The statutory history, however, again presents no evidence that Congress was aware that the injunction section of the Act could or would be used to impose prior restraints on newspapers or magazines.

D. Conclusion

Deciphering Congressional intent is always a precarious task. Language is often ambiguous, statutes may be poorly drafted, and legislators rarely contemplate every application of their words. Yet several general conclusions can be drawn from the language and legislative history of the information control provisions of the Atomic Energy Act. First, though the definition of Restricted Data is broad enough to encompass privately generated atomic energy information, other language in the Act and related statutory materials point to a narrower reading. The evidence that Congress believed Restricted Data was information owned and controlled by the government is considerable. At a minimum, sufficient ambiguity surrounds the intended scope of the Restricted Data concept to invoke the principle of *Greene v. McElroy*,[191] that in the absence of a clear, unequivocal, and

187. *See, e.g., Hearings on S. 1717, supra* note 137, at 117, 155, 165; *Hearings on H.R. 8862 and S. 3323, supra* note 51, at 40, 51-53, 240, 396.

188. *See Hearings on S. 1717, supra* note 137, at 128-34.

189. *See,e.g., Hearings on H.R. 8862 and S. 3323, supra* note 51, at 52, 540-42.

190. *Id.* at 541.

191. 360 U.S. 474 (1959). In *Greene*, the Supreme Court held that the Department of Defense could not fire an employee without affording him the right to confront the sources of derogatory information about him. *Id.* at 508. The court stated that neither

express statement, a congressional act may not be read to authorize governmental action of doubtful constitutionality.[192]

Second, even if the Act does apply to privately developed information, certainly neither DOE nor the NRC have authority to impose security clearance controls over such information. This information is subject only to the espionage controls of the Act — a distinction of considerable significance to private groups working in the atomic energy field.

Finally, the principle of *Greene v. McElroy*[193] also may be applied to the communication/publication problem, though with less force. Although the evidence that Congress intended communication to include publication is strong, Congress did not show "careful and purposeful consideration"[194] — or even awareness — that the Act might be interpreted to authorize prior restraints. In *New York Times Co. v. United States*,[195] the Supreme Court refused to restrain publication of the Pentagon Papers in part because Congress had not passed a precise, narrowly tailored, specifically considered law authorizing such a restraint.[196] For the same reasons, therefore, the federal courts should not read the Atomic Energy Act's definition of communication expansively to include all forms of publication, absent clear statutory language authorizing such an interpretation.

V. Constitutional Issues

If the information controls of the Atomic Energy Act are read to apply to privately generated data, they almost certainly run afoul of the free speech guarantee of the first amendment. Their chief vice is overbreadth. On their face, they authorize the prosecution of or an injunction against communication of all atomic energy information falling within the definition of Restricted Data, if this information is communicated with reason to believe it will harm the United States or advantage a foreign nation. The definition of Restricted Data is so broad[197] and the "reason to believe" culpability standard is so easy to satisfy[198] that public debate concerning atomic energy issues is seriously imperiled. Moreover, the Act authorizes security clearance controls over the communication of Restricted Data without regard to

---

the Congress nor the President had explicitly authorized the Department's proceedings. *Id.*. The court required such authorization to be explicit, especially in areas of doubtful constitutionality. *Id.* at 507.

192. *Id.*.

193. *See* notes 191-92 *supra* and accompanying text.

194. *See* Greene v. McElroy, 360 U.S. at 509.

195. 403 U.S. 713 (1971); *See* notes 228-32 *infra* and accompanying text.

196. *See* 403 U.S. at 720-22 (Douglas, J., concurring); *id.* at 730 (Stewart, J., concurring); *id.* at 740 (White, J., concurring); *id.* at 747 (Marshall, J., concurring).

197. *See* notes 43-50 *supra* and accompanying text.

198. *See* notes 73-74 *supra* and accompanying text.

the speaker's state of mind. [199] No matter what intention a person may have, he may not communicate Restricted Data unless he has a security clearance and then, he may communicate only to persons with like clearances.[200] In sum, the information controls are not narrowly drawn to punish or control only the kinds of speech unprotected by the first amendment,[201] the most relevant of which is speech that poses a clear and present danger[202] of harm to national security.[203]

---

199. *See* notes 75-78 *supra* and accompanying text.

200. *See* notes 75-78 *supra* and accompanying text.

201. Although members of the Burger Court have hinted that a new free speech methodology is on the way, *see* Young v. American Mini Theatres, Inc., 426 U.S. 50, 84 (Stewart, J., dissenting) (1976), the Court continues to apply the so-called categorization test it inherited from its predecessors. *Compare In re* Primus, 436 U.S. 412 (1978) *with* Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447 (1978). Under the categorization test, speech is absolutely protected against content-based regulation unless it falls within one of several narrowly defined categories of speech held to be outside the scope of first amendment protection. The categories include obscenity, *see, e.g.,* McKinney v. Alabama, 424 U.S. 669, 673-74 (1976) (obscene materials are beyond the first amendment), defamatory falsehoods, *see, e.g.,* Time, Inc. v. Firestone, 424 U.S. 448, 457 (1976) (inaccurate and defamatory reports of facts deserve no first amendment protection), and speech that presents a clear and present danger of producing a substantive harm, *see, e.g.,* Schenck v. United States, 249 U.S. 47, 52 (1919) (original formulation of the clear and present danger doctrine).

202. The clear and present danger doctrine is an infrequently invoked, but still viable, first amendment tool that permits courts to distinguish between the protected advocacy of ideas and the unprotectd incitement of violence. It has had an uneven, checkered development but, in the Warren Court era, finally emerged as an effective and broad protection of so-called subversive speech. *See generally* Brandenberg v. Ohio, 395 U.S. 444 (1969). Regulation of this form of speech is permitted only if it is "directed to inciting or producing imminent lawless action" and is "likely to incite or produce such action." *Id.* at 447. Essentially three facts must coexist before expression is deemed a clear and present danger. The words of the speaker, objectively viewed, must be (1) intended to produce (2) and likely to produce (3) imminent violent or unlawful activity. A fourth factor, implicit in the doctrine but never explicitly set forth, is that the harm must be serious. Although questioning its relevance in certain contexts, and misapplying it on occasion, *see, e.g.,* Landmark Communications, Inc. v. Virginia, 435 U.S. 829, 842-45 (1978); Madison School Dist. v. Wisconsin Employment Relations Comm'n, 429 U.S. 167, 173-74 (1976), the Burger Court has made no attempt to abandon the clear and present danger doctrine.

Commentators have argued that the categories of unprotected speech are too broad, *see, e.g.,* T. EMERSON, THE SYSTEM OF FREEDOM OF EXPRESSION 7, 16 (1970) (all expression which is not action should be protected), and too narrow, *see, e.g.,* Bork, *Neutral Prinicples and Some First Amendment Problems*, 47 INDIANA L.J. 1, 8-9 (1971) (only purely "political" speech should be protected, "speech concerned with governmental behavior, policy or personnel" but not "scientific, educational, commercial or literary expressions as such").

203. With respect to the Atomic Energy Act, the question is whether communication of privately developed atomic energy information presents a clear and present danger of immediate and serious harm to national security. More specifically, taking the *Progressive* case as an illustrative fact scenario, the crucial issue is whether publication of how to build a thermonuclear weapon presents a clear and present danger of immediate and serious harm to national security.

As a beginning, it should be apparent that this kind of communication can not be an incitement in the usual sense. It is not advocacy of action, *see, e.g.,* Yates v. United States, 354 U.S. 298, 320 (1957), nor an exhortation of any kind. *See generally* Brandenberg v. Ohio, 395 U.S. 444 (1969). The speaker or publisher is simply setting out the facts and, at worst, is indifferent to what action may follow. To amount to an incitement, then, the communication would have to be viewed as so facilitative of harm that it was no different from incitement. To be more direct, the communication must be so facilitative of harm that it is equivalent to it. In this view, telling someone how to make a nuclear weapon is equivalent to giving that person a bomb already constructed.

Before factually considering whether these assertions are true, some immediate legal objections arise. First, the scope of a facilitation rule would be hard to confine. It could include publication of scientific formulas of any number of chemicals, such as

The issue of prior restraint is especially troublesome. If the Atomic Energy Act permits the government to enjoin the publication of any newspaper or magazine article because it contains information within the definition of Restricted Data, this broad statutory authorization directly contravenes the constitutional precept that no national security prior restraint may issue unless the government convincingly proves that publication "will surely result in direct, immediate, and irreparable damage to our Nation."[204]

A. Overbreadth

Congress has broad power to protect national security and provide for the common defense.[205] This power undoubtedly includes the authority to establish a classification scheme over government documents and to regulate expression in certain circumstances. By relying on its interest in national security to enact the information control provisions of the Atomic Energy Act,[206] Congress assumed a relationship between communication of atomic energy information and serious harm to the nation. Of course, it is possible that certain privately developed atomic energy information, if made available to

---

those for nerve gas or napalm. It might even embrace a set of instructions for making Molotov cocktails. Moreover, no logical limit would confine the rule to information that facilitates the construction or use of weapons. It could extend as well to any aids or guides about how to succeed in crime affecting national security, such as sets of instructions for effecting a kidnapping or hijacking or a discussion of the latest and most successful terrorist methods.

Second, a facilitation rule would completely attenuate the causality requirement in the clear and present danger test. Making something easier for someone to do is not the same as causing him to do it. Giving someone an idea to act in a certain way is not the same as inciting that action. Assuming that the publication of certain information might present serious hazards to public safety by giving others the capacity to inflict harm, the clear and present danger doctrine, and indeed first amendment values, require that the causal connection between the publication and the harm be quite direct. *Cf.* Scanlon, *A Theory of Freedom of Expression*, 1 PHIL. & PUB. AFF. 204, 211-15 (1972) (explaining the different routes by which expression can lead to action). For example, in United States v. Featherson, 461 F.2d 1119 (5th Cir.), *cert. denied*, 409 U.S. 991 (1972), the Fifth Circuit upheld the constitutionality of a Florida statute that made it unlawful to teach or demonstrate to any person the use, application, or making of any firearm or explosive or incendiary device with knowledge or reason to know that the firearm or device would be unlawfully used in or to further a civil disorder. The court upheld the conviction of the defendants under the statute on evidence that showed a direct link between the dissemination of information and immediate and serious harm. Specifically, the record showed that the defendants were leaders of a cohesive organized group known as the Black Afro Militant Movement, that they instructed members on how to make and assemble explosive and incendiary devices, and that this group was standing ready to strike transportation and communication facilities at a moment's notice. *Id.* at 1122-23.

Leaving the difficult legal issues of scope and causality aside, two questions remain: is publishing how to make an H-bomb equivalent to giving the H-bomb to a foreign country and, if so, will it directly lead to immediate and serious harm to national security? The answers depend on a number of factors. *See* notes 241-44 *infra* and accompanying text (answering both questions in the negative).

204. New York Times Co. v. United States, 403 U.S. at 730 (Stewart, J., concurring); *see* notes 228-36 *infra* and accompanying text.

205. U.S. CONST. art. I, § 8, cl. 1.

206. *See* 42 U.S.C. § 2161 (1976).

terrorists or foreign governments, could seriously harm the United States. Because widespread dissemination of atomic energy information has already occurred[207] and because privately developed atomic energy information is probably easily duplicated,[208] the amount of atomic energy information capable of causing serious harm is quite small. Yet, the scope of the information control provisions is not limited to information that, if communicated, will present or will likely present a clear and present danger of harm to national security. The law simply assumes that every piece of atomic energy information is *per se* harmful. The communication of all atomic energy information, whether harmful, helpful, or innocuous is prohibited.[209]

This sweeping rule of prohibition undermines one of the most significant developments in American constitutional law: the idea that individual rights are best protected by legislation that is specifically and narrowly tailored to an appropriate governmental objective.[210] The idea has particularly strong roots in first amendment doctrine.[211] In *United States v. Robel*,[212] for example, the defendant was prosecuted under a federal statute[213] that prohibited employees in certain defense plants from continuing to work once they had knowledge that they belonged to "communist action" organizations as defined by the Subversive Activities Control Board.[214] In holding the statute unconstitutional, the Supreme Court did not deny that protecting against sabotage in defense facilities was a proper governmental purpose.[215] Nor was the Court concerned with whether Congress could reasonably have found that communists might use their positions to engage in sabotage.[216] Rather, the Court was "concerned solely with determining whether the statute . . . has exceeded the bounds imposed by the Constitution when First Amendment rights are at stake."[217] The Court noted that it had only to determine whether Congress had adopted a constitutional means to achieve an admittedly legitimate goal.[218] The Court held that "the Constitution requires that the conflict between congressional power and individual rights be accomodated by legislation drawn more narrowly to avoid the conflict."[219]

---

207. *See* notes 266-77 *infra* and accompanying text.
208. *See* notes 278-79 *infra* and accompanying text.
209. *See* notes 72-78 *supra* and accompanying text.
210. *See, e.g.*, Gunther, *Foreword: In Search of Evolving Doctrine on a Changing Court: A Model for a Newer Equal Protection*, 86 HARV. L. REV. 1, 20-24 (1972). *See generally* United States v. Carolene Products Co., 304 U.S. 144, 152 n.4 (1938).
211. *See, e.g.*, Spence v. Washington, 418 U.S. 405, 414 n.9 (1974); United States v. O'Brien, 391 U.S. 367, 381-82 (1968); Shelton v. Tucker, 364 U.S. 479, 488 (1960); Cantwell v. Connecticut, 310 U.S. 296, 311 (1940). *See also* Ely, *Flag Desecration: A Case Study in the Roles of Categorization and Balancing in First Amendment Analysis*, 88 HARV. L. REV. 1482, 1483-84 (1975).
212. 389 U.S. 258 (1967).
213. *Id.* at 259-60. The defendant was prosecuted under the Subversive Activities Control Act of 1950, § 5(a)(1)(D), 50 U.S.C. § 784(a)(7)(D) (1976).
214. 389 U.S. at 259-60.
215. *Id.* at 264.
216. *Id.* at 266-67.
217. *Id.* at 267.
218. *Id.* at 268 n.20.
219. *Id.*

Robel, and cases decided in its wake,[220] indicate that the fundamental vice of an overbroad statute is that both the person immediately affected, as well as others who may want to express ideas, are inhibited or "chilled" from exercising their constitutional rights. The atomic energy information controls have recently been applied only against *The Progressive*[221] magazine, but the law also inhibits the expression of scientists, researchers, and anyone who works with atomic energy information. Worse, by potentially cutting off almost all communication involving atomic weapons, the statute necessarily inhibits politically relevant discussion about whether the government is adequately protecting against nuclear proliferation.[222]

B. Prior Restraint

Ultimately, the breadth of the concept of Restricted Data also condemns the use of the information controls to restrain publication of atomic energy information. Prior restraints are highly disfavored and carry a heavy presumption of unconstitutionality.[223] Although not absolutely prohibited, they are "recognized only in exceptional cases."[224] If the Atomic Energy Act permits prior restraints, injunctions could issue prohibiting the publication of articles about the Salt II Treaty, speculation that the United States is developing new or dif-

220. *See, e.g.*, Gooding v. Wilson, 405 U.S. 518, 520-21 (1972). *See also* Note, *The First Amendment Overbreadth Doctrine*, 83 HARV. L. REV. 844 (1970). The Burger Court has not recast the basic and classic formulation of the overbreadth doctrine that a statute is facially invalid if it "does not aim specifically at evils within the allowable areas of [government] control but, on the contrary, sweeps within its ambit other activities that . . . constitute an exercise of freedom of speech." Thornhill v. Alabama, 310 U.S. 88, 97 (1940). It has, however, made explicit the idea that a law should not be held facially invalid unless the chill on deterrence of protected activities is substantial. *See* Broadick v. Oklahoma, 413 U.S. 601 (1973). In *Broadick*, the Court held that when a statute regulates conduct involving more than "pure speech", its overbreadth must "not only be real, but substantial as well, judged in relation to the statute's plain legitimate sweep." *Id.* at 615.

221. The Justice Department has indicated that it may file criminal charges against persons involved with the recent publication of "secret" atomic energy information in the MADISON PRESS CONNECTION. *See* note 11 *supra*.

222. Even if it were true that one need not have the details of bomb manufacture to discuss nuclear weapons issues, the point is that the Act does not limit its reach to such matters but, rather, cuts broadly into all information related to atomic energy and atomic weapons. Consider, for example, a recent case in which residents of Hawaii sued, unsucessfully, to enjoin the United States from using facilities at the Pearl Harbor Naval Base for the storage of nuclear weapons. Catholic Action of Hawaii v. Brown, 468 F. Supp. 190, 191 (D. Hawaii 1979). The citizens' group suit was aimed at forcing the Navy to submit an environmental impact statement on the weapons storage project. The district court held, however, that the submission of an environmental impact statement was not required because it would conflict with the Restricted Data provisions of the Atomic Energy Act. *Id.* at 193. Although the case involves government information as opposed to privately developed information, it nicely illustrates one way in which the Atomic Energy Act operates to shield government action from public scrutiny.

223. *See, e.g.*, New York Times Co. v. United States, 403 U.S. 713, 714 (1971); Organization For A Better Austin v. Keefe, 402 U.S. 415, 419 (1971).

224. *See* Near v. Minnesota, 283 U.S. 697, 716 (1931).

ferent nuclear weapons, evidence that nuclear reactors are unsafe, a new discovery that would make the production of nuclear power safer, or studies showing that workers in nuclear plants or in weapons development programs run higher risks of cancer. All of these articles would contain information "concerning" the design, manufacture, or utilization of atomic weapons or the production or use of enriched uranium or plutonium in the production of energy.[225] The publisher probably would have reason to believe that publication will harm the United States or secure an advantage to a foreign nation — even if that advantage is only knowing what the United States knows or confirming what the foreign country already knew.[226] If security clearance controls apply to privately developed information falling within the definition of Restricted Data, then no such information could ever be generally published, not because of reason to believe a foreign nation would be advantaged, but because readers would not have the requisite security clearance.[227] The government might respond to this by saying that it has not and would not apply the act so broadly. The evil of such a statute, however, lies not necessarily in what has been done but rather in what could be done.

In *New York Times Co. v. United States*,[228] the single case prior to the Progressive in which the government sought a prior restraint on national security grounds, the Supreme Court adhered to and reaffirmed its view that prior restraints are presumptively unconstitutional and that the virtually total ban against this form of control of expression has only extremely narrow exceptions.[229] The government claimed that the *New York Times* and the *Washington Post* had published and were about to publish top secret documents that would allegedly prolong the Viet Nam War, embarrass the United States and other governments, lead to the death of soldiers and government agents, and destroy sensitive foreign alliances and contacts.[230] Despite Justices Stewart and White's concern that, in the national interest, some documents should not be published,[231] and Justice Blackmun's fear that publication could result in the death of soldiers, the destruction of alliances, and the greatly increased difficulty of negotiation with our enemies, [232] the Court, in a six to three decision, denied the government's request for an injunction.[233]

Although no single test emerged from the separate opinions of the majority members,[234] a majority agreed that a prior restraint is justi-

225. *See 42 U.S.C. § 2014(y) (1976); notes 32- 50 supra* and accompanying text.
226. *See* Edgar & Schmidt, *supra* note 73, at 987-88.
227. *See* notes 75-78 *supra* and accompanying text.
228. 403 U.S. 713 (1971) (per curiam).
229. *Id.* at 714 (per curiam).
230. Brief for the United States in the Supreme Court at 6, 16-18, 23-25, New York Times Co. v. United States, 403 U.S. 713 (1971).
231. 403 U.S. at 728-29 (Stewart, J., concurring); *id.* at 730-40 (White, J., concurring).
232. *Id.* at 763 (Blackmun, J., dissenting).
233. *Id.* at 714 (per curiam).
234. The judgment of the Court was announced in a brief per curiam opinion. Justices Black, Douglas, Brennan, Stewart, White and Marshall wrote separate concurrences and Chief Justice Burger and Justices Harlan and Blackmun wrote separate dissents.

fied, if at all, only on a government showing that publication will immediately and inevitably cause grave harm to national security.[235] Further, the government must prove these harmful effects by clear and convincing evidence.[236] To show that publication could, might or may cause serious harm would not be enough to meet these strict standards.

If the Atomic Energy Act permits prior restraints, it permits them in circumstances far broader than those narrowly and specifically identified in *New York Times*. Even in the *Progressive* case, which the government undoubtedly believes to be its strongest possible prior restraint case, the "exceptional" circumstances that would justify a national security prior restraint are absent. The trial court found only that the magazine article "*could* accelerate the membership of a candidate nation in the thermonuclear club,"[237] that "once basic concepts are learned, the remainder of the process *may* easily follow,"[238] that the article "*could possibly* provide sufficient information"[239] to enable a nation to construct a hydrogen bomb, and that "[p]ublication of the Restricted Data contained in the article *could* materially reduce the time required by certain countries to achieve a thermonuclear capability."[240]

Several general observations can be made about the factual weaknesses in the government's case over and above these conclusions drawn by the trial court. The basic question is whether publication of information on how to make an H-bomb is equivalent to giving the H-bomb to a foreign country. Will publication directly cause immediate and serious harm to national security? The answer depends on a number of factors. First, is the information already publicly available? If it is — and there is evidence that the information that *The Progressive* wanted to publish was publicly available —[241] the harm existed before publication. Second, even if the information is not publically available, is it readily derivable from public sources? Some assessment must be made of how easy or difficult it would be for another person to put the information together.[242] If the information is readily derivable then the harm, again, existed before publication. Finally, is the theory of how to make an H-bomb the equivalent of having the bomb, or is it at least a significant step in obtaining it? Experts on nuclear proliferation agree that the obstacles preventing

235. 403 U.S. at 730 (Stewart, J., concurring); *id.* at 726-27 (Brennan, J., concurring). Justices Black and Douglas believed that prior restraints were absolutely prohibited. *Id.* at 717 (Black, J., concurring); *id.* at 724 (Douglas, J., concurring).
236. *Id.* at 714.
237. United States v. The Progressive, Inc., 467 F. Supp. 990, 994 (emphasis added).
238. *Id.* (emphasis added).
239. *Id.* at 993 (emphasis added).
240. *Id.* at 999 (emphasis added).
241. *See* notes 266-73 *infra* and accompanying text.
242. *See* notes 272-75 *infra* and accompanying text.

production of a nuclear weapon are not informational.[243] Rather, they lie in acquiring the cadre of skilled scientists needed to reduce the information to application, building the sophisticated and expensive facilities needed for production, and obtaining the necessary plutonium or weapons grade uranium.[244] If this is true, then describing the theory of the H-bomb can not be the equivalent of providing an H-bomb nor will it lead directly and immediately to providing one. Given the trial court's own conclusions and from what is currently known, it appears impossible that any court could find that publication of an article like *The Progressive* article would inevitably lead to great harm to the nation. That the trial court granted an injunction against publication shows quite clearly that the court misapplied the *New York Times* rule.

Although acknowledging that *New York Times* governed,[245] the trial court in fact succumbed to the danger that the *New York Times* test was designed to prevent. Instead of requiring that the government meet its heavy burden of proof with clear and convincing evidence, the court weighed the interests on both sides. It balanced the gravity of the risk, posited to be death from nuclear annihilation, against the importance to the public of knowing the specific details of hydrogen bomb manufacture.[246] With the issue thus presented, the result was a foregone conclusion. Case-by-case determinations of whether the government's or the speaker's interest has more weight or is more important will almost always mean that the infringement on free speech will be upheld. The perceived public interest — peace, order, national security, life — will almost always outweigh a single instance of censorship. When the question is, "in light of the possible harm, do we need to know *that particular information, that specific data*?," the answer will invariably be "no." The *New York Times* rule and the long accepted presumption against prior restraints rest on the realization of the risks involved in arguing freedom of speech from the individual perspective.

Although far from clear, the trial court may have concluded that the injunctive authority granted by the Atomic Energy Act lessened the government's burden of proof below the level articulated in *New York Times*.[247] If this is true, there are two responses to the district court's position. First, statutory authorization should not immunize a prior restraint from constitutional disfavor. This disfavor has strong historical roots,[248] has been consistently expressed in a long line of

243. *See Hearings on S. 2236, supra* note 8, at 259. *See also* notes 271-75 *infra* and accompanying text.

244. *See Hearings on S. 2236, supra* note 8 at 259.

245. *See* United States v. The Progressive, Inc., 467 F. Supp. at 994. The trial court, however, did attempt to distinguish the *New York Times* case. First, it said that the nature of the information in each case was different: the *New York Times* case involved an historical account of United States involvement in Viet Nam and the *Progressive* case, unlike the *New York Times* case, involved a directly applicable statutory authorization of a prior restraint. The court failed to explain whether or why these distinctions may have justified a departure from the *New York Times* rule. *Id.* at 999.

246. *Id.* at 995-96.

247. *Id.* at 994, 996.

248. *See* Grosjean v. American Press Co., 297 U.S. 233, 245-50 (1936); Near v. Minne-

unbroken precedent,[249] and, as a practical matter, is a reaction against the devastating efficiency with which prior restraint suppresses expression.[250] It is also a recognition of the strong tendency of all systems of prior retraints, once established, to expand beyond their original boundaries.[251]

Even in *New York Times*, in which the Justices discussed the possible relevance of congressional legislation to the issues raised by publication of the Pentagon Papers,[252] no suggestion was made that the existence of such legislation could or would lower the constitutional standard employed by the judiciary to measure the validity of national security prior restraints. Rather, the Justices lamented the lack of congressional guidance and suggested that Congress could, after appropriate fact finding, define a very narrow and specific class of information, disclosure of which in Congress's judgment would lead to grave, immediate, and irreparable harm to the national security.[253] The constitutional standard thus would remain the same. Although the prior restraint may be embodied in a legislative judgment, the legislative judgment itself would remain subject to judicial scrutiny.[254] Justice Harlan was the sole proponent of a very narrow scope of judicial review when issues involving publication of defense information were involved.[255] His view was premised on a general notion

---

sota, 283 U.S. 697, 713-15 (1931); 4 W. BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 151-52 (2d ed. rev. 1872). *See generally* L. LEVY, LEGACY OF SUPPRESSION: FREEDOM OF SPEECH AND PRESS IN EARLY AMERICAN HISTORY (1960).

249. *See, e.g.,* Nebraska Press Ass'n v. Stuart, 427 U.S. 539 (1976); New York Times Co. v. United States, 403 U.S. 713 (1971); Organization For A Better Austin v. Keefe, 402 U.S. 415 (1971); Grosjean v. American Press Co., 297 U.S. 233 (1936); Near v. Minnesota, 283 U.S. 697 (1931).

250. *See* T. EMERSON, THE SYSTEM OF FREEDOM OF EXPRESSION 506 (1970). Professor Emerson put the case best:

> A system of prior restraint is in many ways more inhibiting than a system of subsequent punishment: It is likely to bring under government scrutiny a far wider range of expression; it shuts off communication before it takes place; suppression by a stroke of the pen is more likely to be applied than suppression through a criminal process; the procedures do not require attention to the safeguards of the criminal process; the system allows less opportunity for public appraisal and criticism; the dynamics of the system drive toward excesses, as the history of all censorship shows.

Id. See also .A. BICKEL, THE MORALITY OF CONSENT 61 (1975). Alexander Bickel has stated: "Prior restraints fall in speech with a brutality and a finality all their own. Even if they are ultimately lifted they cause irremedial loss — a loss in immediacy, the impact, of speech . . . . A prior restraint, therefore, stops more speech more effectively. A criminal statute chills, prior restraint freezes." *Id.*

251. *See, e.g.,* T. EMERSON, *supra* note 250, at 9-10.

252. New York Times Co. v. United States, 403 U.S. at 720-22 (Douglas, J., concurring); *id.* at 730 (Stewart, J., concurring); *id.* at 732-40 (White, J., concurring); *id.* at 743 (Marshall, J., concurring).

253. *See* 403 U.S. at 730 (Stewart, J., concurring); *id.* at 732-40 (White, J., concurring); *id.* at 742-44 (Marshall, J., concurring).

254. *Id.* at 730 (Stewart, J., concurring). Justice Stewart noted that "if Congress should pass a specific law authorizing civil proceedings in this field, the courts would likewise have the duty to decide the constitutionality of such a law as well as its applicability to the facts proved." *Id.*

255. *Id.* at 757 (Harlan, J., dissenting).

of judicial deference to presidential judgments in the area of foreign affairs.[256] This was not the view of other members of the Court, however, and the general argument of lack of judicial competence[257] has been rejected before in free speech cases.[258]

The second response to the *Progressive* court's lower standard of proof is that the Atomic Energy Act is not, in any event, the kind of specific, narrowly tailored guidance the Court sought in the *New York Times* case.[259] Returning to the problem of overbreadth, the information controls of the Act, no matter what standard of proof is employed, simply sweep too broadly.[260]

VI. A Policy Perspective

The information control provisions of the Atomic Energy Act are premised, in part, on the idea that secrecy preserves security.[261] The need for secrecy is not limited to weapons design nor is it confined to so-called "census" secrets, such as number variety, or location of weapons. It covers a vast amount of atomic energy data in both military and non-military spheres. If the government's position is correct,

256. *Id.* at 756 (Harlan, J., dissenting). At least two commentators have expressed agreement with the view that in the area of national security, the judiciary lacks the competence to fashion appropriate and satisfactory constitutional rules. These two have argued that "[t]he judicial process is not well suited to judge the risks inherent in releasing particular secrets. The task necessarily requires conjectures, and adequate conjectures cannot be made without an overview of the substance and interrelationship of military and diplomatic policy that the judicial process cannot provide. . . ." Edgar & Schmidt, *supra* note 73, at 933 (footnote omitted).

257. *See* note 256 *supra*.

258. *See, e.g.*, Brandenberg v. Ohio, 395 U.S. 444 (1969), *overruling* Whitney v. California, 274 U.S. 357 (1927). *Compare* Chaplinsky v. New Hampshire, 315 U.S. 568 (1942) (Court willing to accept the implied legislative judgment that there is an almost certain link between certain fighting words and the outbreak of violence) *with* Gooding V. Wilson, 405 U.S. 518 (1972) (Court applied a more penetrating scrutiny and found a state law proscribing the use of opprobrious words and abusive language overbroad).

Of course, the problem of judicial competence may be the most troubling aspect about the *Progressive* case or, indeed, any case in which a court is asked to review, or second guess, an executive judgment that certain actions must be taken to protect the national security. The adjudicatory process is probably ill- suited to informed decision-making in this area, but what is the alternative? To refuse to decide such cases is only to decide that the decisions will be made elsewhere. In that event, the judiciary can either treat these issues as a species of political question and withdraw completely, *see, e.g.*, A. BICKEL, THE LEAST DANGEROUS BRANCH 184 (1962), or it can follow a course of limited review and vest governmental determinations in this area with a presumption of validity. In either event, given the government's tendency to see national security implications in an enormously wide range of actions, the courts would abdicate a broad measure of their special responsibility to preserve and protect individual rights. In this regard, the comments of Justice Jackson are instructive:

> [F]reedoms of speech and of press . . . may not be infringed on such slender grounds. They are susceptible of restriction only to prevent grave and immediate danger to interests which the State may lawfully protect. . . .
>
> Nor does our duty to apply the Bill of Rights to assertions of official authority depend upon our possession of marked competence in the field where the invasion of rights occurs. . . . [W]e act in these matters not by authority or our competence but by force of our commissions. We cannot because of modest estimates of our competence . . . withhold the judgment that history authenticates as the function of this Court when liberty is infringed.

West Virginia State Bd. of Educ. v. Barnette, 319 U.S. 624, 639-40 (1943).

259. *See* note 253 *supra*.

260. *See* notes 204-22 *supra* and accompanying text.

261. *See* 42 U.S.C. § 2161 (1976); notes 24-25 *supra* and accompanying text.

it may even include information privately developed, making no distinction between a highly dangerous and sophisticated new technology, and basic scientific and technical data.

The Progressive published its H-bomb article to question the wisdom of attempting to maintain, or purporting to maintain, secrecy over this second kind of information.[262] In its view, there are no basic nuclear energy secrets to be kept, and if the government thinks otherwise, it is either behaving foolishly or trying to divert the public from confronting the real problems of nuclear non-proliferation.[263] To dramatize its point, *The Progressive* detailed the steps of H-bomb construction to prove that one need not have access to classified documents nor a doctorate in physics to make a working bomb.[264]

No matter what one thinks of *The Progressive*'s editorial judgments, the article raises a fundamental question: Does secrecy over privately developed information make any sense? Congress has promised to review this question as a result of *The Progressive*'s actions.[265] It can only be answered in light of two basic observations: 1) the amount of privately developed information that can be kept secret is extremely small, and 2) the costs of maintaining secrecy are extremely high.

With regard to the first observation, privately developed nuclear energy secrets can not include information already in the public domain or information readily derived therefrom because, by definition, a secret is not widely known. In 1954 and afterwards, the United States opened the nuclear energy field to private interests and encouraged nuclear development internationally.[266] Thousands of per-

---

262. THE PROGRESSIVE, May 1979, at 15, 21-22; Knoll, *Nuclear "Secrets"* . . ., Wash. Post, March 13, 1979, at A 17, col. 2.

263. THE PROGRESSIVE, May 1979, at 15, 21-22. THE PROGRESSIVE'S view has been publicly supported by physicists with backgrounds in nuclear weapons and arms control policy. *See, e.g.*, N.Y. Times, Oct. 8, 1979, at A 18, col. 3.

264. *See* Wash. Post, Mar. 13, 1979, at A 17, col. 2. THE PROGRESSIVE stated that its purpose:

> is not merely to demonstrate that there is no rational justification for the secrecy mystique that the government has invoked, but also to disseminate information that is, in our judgement, indispensible if Americans are to make informed decisions on urgent issues of public concern — such issues as potential environmental damage, occupational health and safety risks, arms control and disarmament negotiations and federal spending priorities.

Id. See also Wash. Post, Mar. 28, 1979, at A 23, col. 2.

265. N.Y. Times, May 18, 1979, at A 12, col. 1; Wash. Post, May 18, 1979, at A 1, col. 1.

266. *See Bulletin of the Atomic Scientists*, March 1978, at 28. The government's efforts fell under the Eisenhower program known as "Atoms for Peace". The objective was to give other countries information sufficient to exploit the commercial use of nuclear energy. Although information about weapons design and manufacture was not shared under this program, the basic information needed for commercial activity included certain data transferable to military application. *See Hearings on S. 897 and S. 1432 Before the Senate Subcomm. on Energy Research and Development*, 95th Cong., 1st Sess. 84 (1977) (testimony of Myron Kratzer, International Energy Ass'n) (hereinafter cited as *Hearings on S. 897 and S. 1432*). *See* NUCLEAR ENERGY POLICY GROUP, NUCLEAR POWER ISSUES AND CHOICES 275 (1977). *See generally* Wohlstetter, *Spreading the Bomb Without Quite Breaking the Rules*, 25 FOREIGN POLICY 88 (1976-77).

sons were given access to Restricted Data, and free, worldwide exchange of specified nuclear information among scientists and officials began.[267] The result is that today a spectacular amount of nuclear energy literature is freely available.[268] To illustrate, information about fission bombs[269] is so comprehensive that a recent article concluded that "all the basic information for the design and construction of a wide variety of fission explosives has now been published in the open technical literature."[270]

Last year the Senate Committee on Governmental Affairs held hearings on terrorism and, in that regard, considered DOE practices regarding protection of nuclear weapons "secrets."[271] The testimony made it clear that the basic theory and design of nuclear weapons, including the hydrogen bomb, can and has been gleaned from pub-

---

267. *See Hearings on S. 897 and S. 1432, supra* note 266, at 84. The United States even trained 169 foreign nationals, now working in their own countries, to use and apply the United States's reprocessing technology to separate plutonium from fission products in irradiated fuel. Because nuclear weapons can be made from small amounts of plutonium, restrictions on the further dissemination of reprocessing technology would be ineffective in reducing the danger of nuclear proliferation made possible by earlier programs. *Id. See generally Wohlstetter*, note 266 *supra*.

268. *Id. See* Nuclear Energy Policy Group, *Nuclear Power Issues and Choices*, at 277 (1977). Even without the United States's willingness to share atomic energy information, other nations probably could have or would have acquired the information anyway. First, secrets often leak or, if they are important enough, are stolen. More fundamentally, however, basic scientific information about how nuclear fission or fusion occurs, like any other basic information about the physical world, can not really be "secret." If someone discovers a certain scientific principle or phenomenon, he can not truly keep it secret because others remain free to discover the very same principle or phenomenon. The original discoverer can only refuse to disclose what he has learned. As a practical matter, an original discovery may be tantamount to having a secret if the time it takes to rediscover the principle is anything approaching eternity. In all but a few highly exceptional cases, however, rediscovery of basic scientific and technological advances can be expected either simultaneously or in a very short period. This is so because virtually all science and technology is an extension of discoveries previously made and because the general principles underlying any particular development are likely to be widely known. Indeed the inevitable interchange of scientific information coupled with intelligence activities ensures, contrary to public perception, that no country could carry a weapons research project to conclusion in utter secrecy. Even with respect to a society as closed as the Soviet Union, intelligence experts can describe the direction of weapons research, indicate the probable stage of development, and even predict ultimate capabilities.

In most cases, therefore, the most that can be gained from keeping a scientific discovery "secret" is a small time advantage over a nation's competitors. Even such a minimal advantage, however, is arguably important and, in rare situations, it may prove highly valuable to a nation's defense or to its foreign policy. For example, the United States had a temporary monopoly over atomic weapons at a crucial period in world history. It is not too speculative to suggest that, had Germany or Japan been in the United States's position, a far different world order might have resulted. Or, consider the importance of even a temporary monopoly over new forms of warfare that would make the nuclear variety obsolete. Both of these examples, however, are of the rare sort involving original discovery in a completely new field, a state of the world that has long ceased to exist with respect to atomic energy.

269. Fission bombs, often called atomic bombs, derive their explosive energy from the uncontrolled splitting of the nuclei of certain fissionable materials, principally isotopes of uranium and plutonium. The bombs dropped on Hiroshima and Nagasaki were fission bombs. Fusion bombs, often called hydrogen bombs, derive their explosive energy, which is many times greater than that of an atomic bomb, from the joining of the nuclei of certain light isotopes to produce a more massive one. An atomic bomb provides the tremendous energy needed to trigger the hydrogen bomb, *i.e.*, to fuse the hydrogen nuclei. *See* NEWSWEEK, Oct. 19, 1953, at 34.

270. BULLETIN OF THE ATOMIC SCIENTISTS, March 1978, at 28. *See* Taylor, *Nuclear Safeguards*, 25 ANNUAL REVIEW OF NUCLEAR SCIENCES 407-21 (1975).

271. *See Hearings on S. 2236, supra* note 8, at 249-308.

licly available information.[272] The real obstacles that a nation desiring to acquire nuclear weapons faces are not theoretical or informational.[273] These countries need the wherewithal, — *i.e.*, money, industrial capability, and experience — to manufacture a weapon.[274] Most important, they need nuclear fuel — plutonium or weapons-grade uranium.[275]

During the *Progressive* litigation, the government admitted that it had declassified and placed on the public shelves documents that contained precise details of the design of the hydrogen bomb and a description of the devices that trigger it.[276] Indeed, because nuclear information is so widely available, many proponents of nuclear nonproliferation do not focus at all on information controls. Rather, they argue for materials controls and international agreements.[277]

---

272. *See id.*

273. *See id.* at 259, 285; M. WILLRICH & T. TAYLOR, NUCLEAR THEFT: RISKS AND SAFEGUARDS, 6 (1974).

274. *See Hearings on S. 2236, supra* note 8, at 259; Nuclear Power Issues and Choices, *supra* note 266, at 277-81. The trial court in the *Progressive* case recognized that information alone is not enough to enable a country to construct a hydrogen bomb. The court stated:

> Does that article provide a "do-it-yourself" guide for the hydrogen bomb? Probably not. A number of affidavits make quite clear that a *sine qua non* to thermonuclear capability is a large, sophisticated industrial capability coupled with a coterie of imaginative, resourceful scientists and technicians. One does not build a hydrogen bomb in the basement.

467 F. Supp. at 993. The current "classic" example of the relative unimportance of publicly available bombmaking information is Pakistan. Notwithstanding its possession of sufficient information about how to build a bomb, Pakistan has only advanced toward actual manufacture by acquiring, sometimes surreptitiously, the sophisticated equipment and machinery needed for its project. *See* N.Y. Times, Aug. 24, 1978, at 43, col. 1; *id.*, Jan. 27, 1978, at 5, col. 1. Pakistan, like India before it, used its "peaceful" nuclear power program as a subterfuge to obtain the indispensible, and probably otherwise unobtainable, nuclear weapons equipment. Pakistan denies it is building a nuclear weapon. *Id.*, Apr. 4, 1980, at A 1, col. 5; Apr. 9, 1979, at A 1, col. 2.

275. *See* NUCLEAR POWER ISSUES AND CHOICES, *supra* note 266, at 277-31. Plutonium exists in nature only in minute quantities. It is a by-product of certain atomic reactions. Because producing plutonium requires both a nuclear reactor and a nuclear waste reprocessing capability, it is not easily obtainable. Uranium does occur naturally, but the fissionable isotopes occur in such minute quantities that, as an energy source, natural uranium is of little value. Enriching uranium to usable levels requires facilities even more complex than those required to generate and isolate plutonium. Only a very few nations have the capability to produce either. *See* Gilinsky, *Military Potential of Civilian Nuclear Power*, in NUCLEAR PROLIFERATION: PROSPECTS FOR CONTROL 41 (1970).

Weapons-grade materials are controlled by a handful of nations, including, obviously, the United States and the Soviet Union. Unless these nations donate these materials for political reasons, or lose them by theft, or allow nations such as Pakistan and India to obtain them under the pretext of "peaceful" nuclear power programs, there is, as a practical matter, no way that other nations or subnational organizations such as terrorists groups, can construct nuclear weapons — no matter how much theoretical and design information they possess. *See Hearings on S. 2236, supra* note 8, at 259, 28586, 304-05; A. GUHIN, NUCLEAR PARADOX SECURITY RISKS OF THE PEACEFUL ATOM 26-27 (1976).

276. N.Y. Times, June 9, 1979, § L, at 14, col. 1; Wash. Post, June 9, 1979, at A 1, col. 6.

277. *See, e.g.*, A. GUHIN, *supra* note 275, at 37-66; *Hearings on S. 897 and S. 1432, supra* note 266, at 92-93 (testimony of Dwight Porter, International Government Affairs, Westinghouse Electrical Corp.)

As to the second relevant observation, secrecy over privately developed information generally must be limited because, as with all secrecy, enforcement is effective only in small doses. As Justice Stewart observed in the *Pentagon Papers* case, "[w]hen everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self- protection or self-promotion".[278] Ironically, though, keeping all privately developed information secret would necessarily require an impossibly broad monitoring program. The government would have to review all research projects, all industry developments, all newspaper articles, and all individual speculations to see whether they contained Restricted Data. Anything less would make enforcement a hit or miss proposition dependent on the private person somehow giving notice to the government of his possession of restricted information.[279]

It is understandable that, in 1946, Congress did not exempt information readily discoverable from or freely available in the public literature from secrecy controls because, at that time, all important nuclear energy information was under government control.[280] That assumption is no longer valid. What has not changed is that governmental secrecy exacts high costs in a democratic society. The costs are especially high when the government imposes secrecy on privately developed information. If, as Justice Douglas stated, "[s]ecrecy in government is fundamentally anti-democratic"[281] then, government secrecy over a private person's ideas and communications is tyrannical. It is based on the discredited principle that national security is enhanced more by the suppression of ideas than by the vigorous and free interchange of scientific and technological developments.

Secrecy limitations seriously impair scientific progress by chilling or actually preventing scientific inquiry into fundamental questions, the answers to which may or may not be used militarily.[282] All science proceeds incrementally and builds on what has come before. The thousands of scientific journals on library shelves testify to the importance of knowing the latest experiments and theories in a given field.[283] Secrecy over basic scientific and technological information freezes the ability to go beyond current scientific knowledge. Ultimately, secrecy impairs the United States ability to remain a world

278. New York Times Co. v. United States, 403 U.S. at 729 (Stewart, J., concurring).

279. As indicated, THE PROGRESSIVE article probably would have gone to print without any government review had not the magazine and one recipient of an advance copy brought it to the attention of Energy Department officials. *See* note 92 *supra*.

280. *See* notes 22-26 *supra* and accompanying text.

281. New York Times Co. v. United States, 403 U.S. at 724 (Douglas, J., concurring).

282. *See, e.g., Hearings on S. 1717, supra* note 137, at 155, 277. This theme was sounded repeatedly in the testimony of the atomic scientists who testified on atomic energy legislation in 1946. *Id.* Albert Einstein once said, "[t]he progress of science presupposes the possibility of unrestricted communication of all results and judgments — freedom of expression and instruction in all realms of intellectual endeavor".A.L. MACKAY, SCIENTIFIC QUOTATIONS 51 (1977), *quoting* A. EINSTEIN, OUT OF MY LATER YEARS (1950).

283. *See, e.g.,* HARVARD UNIVERSITY LIBRARY, CURRENT JOURNALS IN THE SCIENCES (6th ed. 1975). This publication lists over 7,100 entries.

leader in the nuclear technology field. Not only will United States scientists be inhibited in their research, but also other countries will move quickly to assume a nuclear role that the United States is either unwilling or unable to assume.[284]

Secrecy also works in a less direct but equally negative way by contributing to the public perception that nuclear energy data is not to be known or questioned or that nuclear energy matters are to be left to government experts.[285] This renders the average citizen unable to judge whether governmental action is wise or foolish.[286] Governmental preoccupation with secrecy may also serve to deflect the public's attention from more fundamental questions and insulate decisionmakers from criticism.[287] Finally, government secrecy over privately developed information creates a precedent for suppression that can be used to support like measures in other scientific and research fields.[288]

Against this background, the benefit of keeping privately developed information secret is particularly hard to discern. If a private citizen can derive the basic theory and design of a nuclear weapon, a law preventing communication will not change the fact that others could similarly derive the information. Moreover, if A can do it, then B can do it, and B may not be a United States citizen. Arguably, at least, the nation's security would be better served by knowing that such derivations are possible. Efforts could then be focused on more effective ways of limiting proliferation of nuclear weapons.

Meaningful and effective information controls require that the gov-

---

284. *See Hearings on S. 897 and S. 1432, supra* note 266, at 93, 96. This latter development can be readily seen by the expanding role assumed by France and Germany in supplying reprocessing technology to other nations in the absence of the United States willingness to serve as a supplier. *Id.*

285. *See* H.P. GREEN & A. ROSENTHAL, GOVERNMENT OF THE ATOM: THE INTEGRATION OF POWERS 199-201 (1963).

286. *See, e.g.*, Catholic Action of Hawaii v. Brown, 468 F. Supp. 190, 193 (D. Hawaii 1979) (nuclear weapons storage project exempt from environmental impact statement requirements); Ruebhansen & von Mehren, *The Atomic Energy Act and the Private Production of Atomic Power*, 66 HARV. L. REV. 1450, 1482-83 (1953); Marks, *The Atomic Energy Act: Public Administration Without Public Debate*, 15 U. CHI. L. REV. 839, 841-43 (1948).

287. *See* Marks, *supra* note 286, at 841-43. For example, only recently it has come to light that the government withheld information and purposefully confused the public about the effect of radioactive fallout and other ills associated with above-ground nuclear weapons testing conducted during the 1950's and 1960's. *See* N. Y. Times, May 13, 1979, at A 1, col.5. Similarly, particularly since the incident at the Three Mile Island Power Plant, questions have been raised about the candor and completeness of government disclosures about the safety and reliability of nuclear facilities. *See, e.g.*, N.Y. Times, May 8, 1979, at A 1, col.5; *id.*, Apr. 13, 1979, at A 1, cols. 1-2; *id.*, Apr. 4, 1979, at A 16, cols. 1-2.

288. *See, e.g.*, Green, *The Recombinant DNA Controversy: A Model of Public Influence*, BULLETIN OF THE ATOMIC SCIENTISTS, Nov. 1978, at 12. Professor Green specifically discusses the parallel between attempted regulation of DNA research and control over atomic energy research. *See also* T. EMERSON, THE SYSTEM OF FREEDOM OF EXPRESSION 9-11 (1970) (the dynamics of articulating and applying restrictions on freedom of speech necessarily result in greater or more widely applicable restrictions).

ernment recognize, as far as possible, which atomic energy information is or is not publicly available or readily derivable. It should then isolate very limited and specific areas of militarily important developing technologies[289] and, as to these, require that all research be performed under a government license. No need for privately developed information controls would exist because the government would eliminate the private character of this kind of research in the first instance. As a practical matter, this development would mean simply that any corporations working on the forefront of militarily significant nuclear energy projects would have to obtain a government license to proceed. Minimally, however, Congress must take a look at the expansive definition of Restricted Data and confine it to government information that the United States affirmatively determines must be kept secret in the interests of national security.

In sum, the information controls of the Atomic Energy Act, if read in the way the government suggests, make little sense because they sweep too broadly. They exact unnecessary costs by trying to keep secret what is not or can not be secret. A legislative second-look is long overdue.

VII. Conclusion

Serious doubt has existed about the proper scope of the information control provisions of the Atomic Energy Act since the law's enactment in 1946. Do they or do they not authorize the government to impose secrecy on atomic energy information developed, generated, or created by individuals working without government funds and without access to classified government documents? Although there is some support for the view that the act does not apply to privately developed information, the language of the law and the general legislative silence on this question point to an interpretation limiting the act to controls over only government information. Until recently, the inherent uncertainty about the law's scope has commanded little attention. Congress has not been pressed for clarification, and the courts have not faced the issue in litigation.

United States v. The Progressive, Inc. marked the first time the government sought judicial aid in applying the atomic energy information controls to privately developed information. The case promised to be the opportunity to reexamine congressional intent with respect to the scope of the Atomic Energy Act and, once reexamined, to decide that the law applies only to government owned or government generated information. Such a decision would have avoided the serious constitutional and policy objections raised by applying the Act more broadly and would have brought the Atomic Energy Act in line with the historical American practice of applying security controls only to government information.

289. Of course, no clear line can be drawn between information that is useful militarily and information that is useful in peaceful applications. *See Hearings on S. 2236, supra* note 8, at 305. This does not mean, however, that the effort to narrow the reach of the Restricted Data concept should be abandoned.

As it happened, the case proved to be a victory for no one. At the district court level, the government successfully prevented the publication of *The Progressive's* hydrogen bomb article, but its case was mooted and the injunction lifted when essentially the same information appeared elsewhere. Further, though *The Progressive* did ultimately publish the article, it lost the opportunity to challenge the lower court's decision. The public, meanwhile, is left to wonder whether and to what extent the Atomic Energy Act really does permit the government to impose secrecy over a citizen's privately developed information. The district court impliedly held that the Act does reach this kind of information. The court's overall reasoning was so flawed, however, that its conclusions probably would not have been upheld on appeal. Of course, this contention is only speculative. Its persuasiveness is further undercut by knowledge that the *Progressive* case was probably the worst case for testing the proper scope of the Atomic Energy Act, as it involved the release of information about one of the most destructive weapons known. In this regard, public reaction to the case merits some analysis. When *The Progressive* announced it would resist the government's censorship, legal experts and some newspapers were sharply critical.[290] Because the issue was nuclear weaponry, many quickly concluded that the government had a winning case. This conclusion was not startling in and of itself: rather, it was suprising because it was so automatic, so reflexive. These critics undoubtedly did not review the language and legislative history of the Atomic Energy Act, and they could not have

290. Typical of the negative reactions were those printed by the leading papers published in Washington, D.C. The Washington Post called *The Progressive* action "John Mitchell's Dream Case," Wash. Post, Mar. 11, 1979, at A 1, col. 2, and The Washington Star described it as a "flawless case for censors," Wash. Star, Mar. 13, 1979, at 8, col. 1. Other papers rallied to *The Progressive's* defense immediately, *see, e.g.,* N.Y. Times, Mar. 29, 1979, at A 22, col. 1. The ranks of supporters steadily increased as the implications of permitting the government to impose secrecy on the discussions and writings of scientists and writers outside of government became clear. Indeed, the New York Times Co., the American Society of Newspaper Editors, the Association of American Publishers, Inc., the National Association of Broadcasters, the Association of American University Presses, the Globe Newspapers Company, the Chicago Tribune Co., the Reporters Committee for Freedom of the Press, the Freedom to Read Foundation, and Scientific American Magazine filed briefs as amici curiae supporting *The Progressive's* position before the court of appeals.

In this regard, the *Progressive* case is a somewhat anomalous prior restraint case in that the passage of time between the trial court's decision and the appellate court's consideration of the matter helped rather than hurt the magazine. Ordinarily, the assumption is that prior restraints are particularly objectionable because, even if ultimately lifted, they cut off the immediacy of speech. *See, e.g.,* A. BICKEL, THE MORALITY OF CONSENT 61 (1975). This objection was not present in the *Progressive* case because the timing of the speech was not a major factor in the controversy. The impact of releasing hydrogen bomb data would be essentially the same whether the release occurred in May or November. Indeed, the government's actions almost insured a wider, more interested audience for the piece. What was occasioned by the months between the trial court's decision and later review was an opportunity for everyone — the press, the public, and the legal community — to take a closer, more rational look at the interests of both sides.

reviewed the sealed record of the case. They simply concluded that discussion of how a hydrogen bomb works, without more, was off limits. This kind of reaction, of course, has no place in adjudication, but it obviously played some part in the trial judge's decision in the *Progressive* case. The court's view of the case as "a stark choice between upholding the right to continued life and the right to freedom of the press"[291] illustrates the point.

In any event, given the unsatisfying conclusion of the *Progressive* litigation, it is imperative that Congress now confront the uncertainty it created when it first wrote a law with such sweeping yet ambiguous information control provisions. As a congressional committee observed, "[h]owever well intentioned, however loosely or intelligently enforced, such a law is a latent danger to the life of this democracy."[292]

291. 467 F. Supp. at 995.
292. H.R. REP. No. 1758, 85th Cong., 2d Sess. 18 (1958).

ATTACHMENT B

96TH CONGRESS
2D SESSION

H. R. 8422

To amend the Atomic Energy Act of 1954 to modify certain provisions relating to restricted data, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

DECEMBER 4, 1980

Mr. MCCLOSKEY introduced the following bill; which was referred to the Committee on Interior and Insular Affairs

---

A BILL

To amend the Atomic Energy Act of 1954 to modify certain provisions relating to restricted data, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That section 11 y. of the Atomic Energy Act of 1954 (42 U.S.C. 2014 y.) is amended to read as follows:

"y. (1) Except as provided in paragraph (2), the term 'Restricted Data' means all data describing—

"(A) the design, manufacture, or utilization of atomic weapons; or

"(B) the production of special nuclear material.

"(2) The term 'Restricted Data' shall not include any information which is declassified or removed from the Restricted Data category pursuant to section 142. Such term shall also not include any information which is, or is derived from information which has been published.

"(3) Notwithstanding paragraph (2), any information which is published and which, but for such publication, would be Restricted Data within the meaning of paragraph (1) shall be treated as Restricted Data for purposes of the initial publication thereof but not for purposes of any subsequent publication.

"(4) For purposes of this subsection, the terms 'publish' and 'publication', when used with respect to any information, refer to any act which has the effect of making such information public."

SEC. 2. Section 224 of the Atomic Energy Act of 1954 (42 U.S.C. 2274) is amended—

(1) by striking out "incorporating Restricted Data—

"a. communicates"

and inserting in lieu thereof: "incorporating Restricted Data communicates";

(2) by striking out the semicolon at the end of subsection a. and substituting a period; and

(3) by striking out subsection b.

○