INFORMATION CONTROL AND ATOMIC POWER DEVELOPMENT*

HAROLD P. GREEN†

The opening of the atomic energy industry to development and exploitation by private enterprise under the Atomic Energy Act of 1954 presents many unique and fascinating problems. Of these, the problems of information control are probably the most interesting and challenging because they represent an experiment without parallel in American law or industry.

The magnitude of the information control problem is implicit in the factual statement of its role in the statutory scheme: private development and exploitation of atomic energy is dependent, to a large extent, upon access to a classified technology controlled by the Atomic Energy Commission in the interest of the common defense and security. Through its control over access to information, the Commission can control entry of firms into the industry, relative competitive positions of competing firms, and proprietary interests in ideas. Even the very study and analysis of a "situation" by a firm to decide whether its resources should be committed to certain uses may require the Commission's approval. The impact of such a framework of government control upon a force such as atomic energy, which is destined to become a basic and pervasive force in the American economy, is obvious. If the present statutory scheme is continued, the growth of atomic energy out of infancy to full maturity is likely to have a profound effect upon many of our basic economic institutions and upon the long-term economic and political structure of American society.

I

THE STRUCTURE OF CONTROL

The statutory framework for atomic energy information control is based upon

*This paper was prepared while the structure of atomic energy information control for private development of civilian applications of atomic energy was in the process of formulation. It is based upon the legacy of eight years' experience under the original Atomic Energy Act, upon the AEC's proposed regulations under the 1954 act, and upon pertinent public statements of knowledgeable AEC officials. Some statements, based upon existing fact when written, may be inaccurate by the time of publication by reason of supervening events; similarly, analysis of the implications of information control may lose validity or take on new proportions. The paper demonstrates, nevertheless, the important and troubling implications stemming from such vast and unique delegation of authority and responsibility to control the flow and use of information. The implications and dilemmas discussed herein will be with us in one form or another so long as our Government continues to impose security-based information control upon democratic society and a free economy.


the concept of "Restricted Data," which is defined in the Atomic Energy Act of 1954 to mean:  

... 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].

As a practical matter, this includes virtually all atomic energy information which the AEC believes warrants protection in the interest of security. It should be noted that the statutory definition embraces all information which falls within its terms, and no action by the AEC is necessary to make such data Restricted Data. The AEC may, thus, control the content of the Restricted Data category only through its authority under section 142 to remove particular data from the category by declassification or transclassification.  

Restricted Data is subject to an array of statutory control provisions. First of all, the AEC is expressly authorized to control the dissemination of Restricted Data in such a manner as to assure the common defense and security. At the same time, the act indirectly imposes upon the AEC the responsibility to exercise its control not only to protect Restricted Data, but also to disseminate Restricted Data, subject to appropriate safeguards, so as to encourage scientific and industrial progress.

The heart of the information control system is the statutory requirement for security clearance of individuals who will have access to Restricted Data. The act contemplates that Restricted Data will be made available only to an individual who has undergone security investigation by the Federal Bureau of Investigation or the Civil Service Commission and who has been granted security clearance upon the AEC's determination that his access to Restricted Data will not endanger the
common defense and security. The AEC is authorized to establish standards and specifications as to the scope and extent of the security investigations which will be required, based upon the sensitivity of the Restricted Data to which access will be permitted.

Section 161(i) of the act authorizes the Commission to prescribe regulations and orders deemed necessary to protect Restricted Data received by any person in connection with activities authorized under the act. In addition, the Commission may exercise information control through the provisions of its contracts and licenses.

The information control system is supported by an array of enforcement provisions. These provisions fall within five distinct categories.

1. Sections 224, 225, and 226 of the act provide severe criminal penalties for espionage-type offenses involving Restricted Data. These penalties do not apply to situations in which there has merely been a violation of information control rules or an unauthorized disclosure of Restricted Data, but only to situations in which there has actually been some kind of espionage-like conduct—i.e., where the act was committed with intent to injure the United States or to aid another nation, or with reason to believe such injury or assistance would result. These provisions are not of particular importance from the standpoint of the impact of atomic energy information control upon industry, since we may assume that very few, if any, individuals in the atomic energy industry would engage in conduct within the ambit of these sections.

2. Of somewhat greater importance is section 227. This section was obviously designed to provide a realistic basis for penal action against persons who disclose Restricted Data outside the circle of authorized persons without any espionage-type intent or state of mind, an offense less serious in scope, iniquity, and consequence than the conduct proscribed under sections 224, 225, and 226.

Section 227 applies to any person who is or has been a government employee, an Atomic Energy Commissioner, a member of the Armed Forces, an employee of a government contractor, an AEC licensee, or an employee of an AEC licensee. Any such person who "knowingly communicates Restricted Data, knowing or having

8§145(a), (b), 68 Stat. 942, 42 U.S.C.A. §2165(a), (b) (Supp. 1954).
1268 Stat. 959, 42 U.S.C.A. §2277 (Supp. 1954). An analogous provision is found in the Internal Security Act of 1950, 64 Stat. 1004, 18 U.S.C. §§793(d), (e) (Supp. 1952), making it an offense punishable by a fine of up to $10,000 and/or imprisonment of as much as 10 years for any person willfully to communicate data relating to the national defense to unauthorized persons. If the data communicated is "information" rather than in tangible or documentary form, an element of the offense is "reason to believe" the information "could be used" to the injury of the United States or to the advantage of another nation.
reason to believe it is Restricted Data, to any person "not authorized to receive Restricted Data pursuant to the provisions of this Act or under rule or regulation of the Commission," knowing or having reason to believe the recipient is "not so authorized to receive Restricted Data," is liable for a maximum penalty of a fine of $2,500.

The efficacy of section 227 is open to serious question. An individual may be "authorized to receive Restricted Data," but yet not authorized to receive specific types of Restricted Data. For example, a recipient may have an "L" clearance, entitling him to access to Confidential Restricted Data, but not to Secret or Top Secret Restricted Data. If an individual subject to section 227 communicated Secret or Top Secret Restricted Data to such a recipient, he probably could not be successfully prosecuted under section 227 even if he admitted knowledge that the recipient was not authorized to receive the data communicated, since it could not be successfully maintained that the recipient was not "authorized to receive Restricted Data." Since the statute and regulations require only security clearance for authorization to receive Restricted Data, successful prosecution would require proof by the Government that the communicator knew or had reason to believe that the recipient was not cleared. It would appear to be an almost impossible task for the prosecution to prove this against any kind of plausible defense. The weaknesses in section 227 could, of course, be easily overcome by a simple amendment changing this element of the crime to knowledge or reason to believe the recipient was not authorized to receive, under the Atomic Energy Act of 1954 or AEC regulations, the Restricted Data communicated.

3. Section 22314 makes it a criminal offense for any person willfully to violate, attempt to violate, or conspire to violate any regulations issued by the AEC pursuant to section 16i(i) of the act to protect Restricted Data. Conviction carries a maximum penalty15 of a fine of $5,000 and/or imprisonment for two years. This provision is the most formidable in the entire enforcement array, and, in effect, gives the AEC's information control system the force and effect of a criminal statute. There is considerable question as to the wisdom of the Congress in delegating to the AEC such broad quasi-legislative authority in so novel a field with so few objective or specifically defined standards.

4. Another potent enforcement tool is provided by section 230,16 which authorizes the issuance of injunctions to restrain violations of or compel compliance with the act and AEC regulations.17

13 It should be noted that under these facts, prosecution could probably be successfully maintained under 18 U.S.C. §793(d) or (e) (Supp. 1952), supra note 12.
15 If, however, the offense is committed with intent to injure the United States or to secure an advantage to any foreign nation, the penalty may be a maximum of a $20,000 fine and/or 20 years' imprisonment. Ibid.
17 The AEC almost had the opportunity in 1950 to test the efficacy of its identical injunction authority under the original Atomic Energy Act of 1946. The publication Scientific American had gone to press.
5. A final enforcement device is the AEC's authority to cancel contracts or revoke licenses for violation of AEC regulations.\textsuperscript{18}

These provisions, taken together, vest the AEC with almost unlimited statutory authority to control dissemination of Restricted Data. The AEC's proposed regulations, issued pursuant to section 161(i), for safeguarding Restricted Data are expressly applicable to "all persons within or under the jurisdiction of the United States."\textsuperscript{10} They provide that "no person possessing Restricted Data shall permit any individual to have access to . . . Restricted Data unless such individual has . . . clearance."\textsuperscript{20} Any person, regardless of the nature of his past or present association, or lack thereof, with the atomic energy program, who discloses Restricted Data to unauthorized persons would probably be in violation of these regulations, and if his action is "willful," he may sustain heavy criminal penalties under section 223.

In addition, if the AEC had advance notice of the proposed publication, it has authority to seek an injunction to restrain the violation. Application of these restrictions to information media, as is entirely possible under the 1954 act, would directly raise a serious question of censorship. It is a striking commentary on our times that legislation authorizing such curtailments of the flow of information has been accepted by the public without resistance.\textsuperscript{21}

It has always been axiomatic that security of information varies inversely with the number of individuals who have access to the information. Accordingly, security programs have traditionally been based upon stringent limitations upon access to classified information. The cardinal principle has been that classified information may be imparted only to those individuals who, of absolute necessity, must

---

\textsuperscript{18} Section 186(a) of the Atomic Energy Act of 1954 authorizes revocation of atomic energy licenses for violation of or failure to observe any of the terms and provisions of the act or of any AEC regulations. 68 Stat. 955, 42 U.S.C.A. §2236(a) (Supp. 1954).


\textsuperscript{20} Id. §95.31.

\textsuperscript{21} The Atomic Energy Act of 1946 did not expressly authorize the AEC to issue information control regulations, and, accordingly, AEC regulations for protecting Restricted Data under the 1946 act lacked injunctive or penal teeth. During consideration of the 1954 act, there was considerable opposition to §227, but no opposition whatever to §161(i), which authorized information control regulations backed by injunctive authority and criminal sanctions, and which was a broader and more effective means, carrying heavier penalties, of accomplishing almost precisely the same object as §227. The principal difference is that prosecution for violation of §161(i) requires a showing of a "willful" violation, while under §227, the offense must be committed "knowingly," with knowledge or reason to believe that Restricted Data is involved and that the recipient was not authorized to receive Restricted Data.
have access in order to perform a function in a government program. The fact that an individual has appropriate security clearance has not entitled him to access to particular classified information unless he also had such a "need to know.

Security clearance was, therefore, granted not to permit general access, but only to permit access to a specified area of information. The AEC security regulations prior to enactment of the 1954 act were based upon strict application of these principles.

It is apparent that under such a philosophy of security, there could be no place for development and exploitation by private enterprise of a classified technology. Private enterprise and personnel of private firms could have access to classified information only to the extent that such access was necessary in order to contribute to a government program in which they were involved. Private exploitation and development necessarily had to await declassification of the pertinent information.

Recent developments under the Atomic Energy Act of 1954, however, have marked a sharp break with the traditional concept of security. Instead of furthering the preservation of security based upon stringently limited access, the act exhorts the Commission to provide for broad dissemination of Restricted Data. The shibboleth of security through limitation of access has been replaced by cautious introduction of the concept that security can be maintained even if large numbers of people have access, if they all are investigated and cleared and subject to realistic criminal sanctions if they violate the security rules. Similarly, the manner in which the AEC is administering the act results in a considerable attenuation of the "need-to-know" doctrine. Restricted Data now is to be made available to private persons even if they do not have a "need to know" in connection with accomplishment of a government program.

The problems of administering the unique information control provisions of the act, of adjusting the necessary departures from traditional security practices to the maintenance of an effective security program, and of administering an information control system in an equitable manner which will preserve free competition and avoid monopoly all present the AEC with a very substantial challenge. The manner in which the Commission proposes to meet this challenge is not yet wholly apparent, since it has not yet issued all pertinent regulations in final form. It is possible, however, on the basis of facts already available, to assess the AEC's general approach to the problem.

Section 7 of Executive Order 10501, 18 Fed. Reg. 7049, 7053 (1953), provides that: "Knowledge or possession of classified defense information shall be permitted only to persons whose official duties require such access in the interest of promoting national defense. . . ."

For example, §195.11(b) of the State Department's Security Regulations provides: "No person is entitled to receive classified . . . information solely by virtue of his official position or by virtue of having been granted security clearance. The 'need to know' doctrine shall be enforced at all times. . . ." See Hearings before a Subcommittee on Reorganization of the Senate Committee on Government Operations on S. J. Res. 21, to Establish a Commission on Government Security, 84th Cong., 1st Sess. 1183, 1237 (1955).

See note 7 supra.
The AEC has adopted regulations dividing Restricted Data into the three categories of relative sensitivity used throughout the Government for security classification of information: Top Secret, Secret, and Confidential. Although the procedures prescribed for the handling of Restricted Data vary with respect to the three categories in accordance with their relative sensitivity, the categories have no significance from the standpoint of the Atomic Energy Act of 1954, since all the information control provisions of the act apply to Restricted Data as such, regardless of the particular classification involved.

Every person who is to have access to Restricted Data must have security clearance. The Commission has, in accordance with section 145(f) of the act, established requirements for two degrees of clearance based upon the category of Restricted Data to which access will be afforded. The "L" clearance will, in so far as concerns private industrial development of atomic energy applications, suffice for access to Confidential Restricted Data and is based upon a National Agency Check. Access to Secret and Top Secret Restricted Data requires a "Q" clearance, based upon a full background investigation by the Civil Service Commission or the Federal Bureau of Investigation. The only difference between an "L" clearance and a "Q" clearance, aside from the difference in access afforded, is in the scope of the required investigation. Although the standards for determining eligibility for clearance may theoretically be applied less stringently for an "L" clearance, where only relatively nonsensitive access is afforded, it is unlikely, as a practical matter, that such a distinction will be drawn.

Under AEC security clearance procedures, an "L" clearance or a "Q" clearance would be revoked or denied only after the individual has been given a statement of the derogatory information and an opportunity for a formal hearing before a personnel security board, with the final clearance determination to be made by the General Manager. These procedures follow the typical pattern of government security adjudications, although in some respects they are more enlightened. Suffice it to say, the procedures fall far short of accepted standards of due process.

It has frequently been said that the Commission's establishment of the "L" clear-
ance creates a so-called “gray area” within which industry would not be bound by clearance procedures as restrictive as if “Q” clearances were universally required.\(^3^1\)

This is an exaggerated statement of the effect of the “L” clearance program. Industry still requires security clearance for access to Restricted Data. There are, however, two differences flowing from the disparity in scope of the investigations required for “L” and “Q” clearances. In the case of a “Q” clearance, the requisite background investigation necessitates a lapse of at least three to four months between the time clearance is requested and the time it is finally granted. In the case of an “L” clearance, the investigation is much briefer, and clearance can be granted within three or four weeks.\(^3^2\) It is this factor of time lag and ease of getting cleared personnel on the job which makes the big difference from industry’s standpoint. A second factor, particularly if industry must bear the costs of clearance of its personnel, is that an “L” clearance is much less expensive.\(^3^3\)

The circle of individuals authorized to have access to Restricted Data embraces two distinct groups. Individuals who participate in government programs relating to atomic energy as government employees or as employees of government contractors who require access to Restricted Data in performance of their duties may have such access after they are cleared. The manner in which Restricted Data is controlled within this part of the circle is a matter of internal government procedure and is beyond the scope of this paper. We are primarily concerned with the second group—individuals who receive access to Restricted Data in order to help them or their employers develop and exploit civilian applications of atomic energy. Restricted Data is made available to these individuals under the AEC’s Access Permit Program.

The Access Permit Program operates at two levels. On the first level, the Commission will provide access to Confidential Restricted Data, on a very broad basis, to any person who can evidence a legitimate economic interest in the information in terms of some potential use or application in his business, trade, or profession.\(^3^4\) A Confidential access permit will permit access to any Confidential Restricted Data relating to civilian uses of atomic energy which is not primarily of military significance.\(^3^5\) Such access would probably be sufficient to enable at least a preliminary judgment as to whether or not the firm or individual concerned wishes to engage in atomic energy activities involving classified technology, and in many instances, it might in itself provide sufficiently complete information to enable com-

\(^3^1\) See, for example, Beckerley, The Impact of Government Information and Security Controls on Competitive Industry, 11 Bull. of the Atomic Scientists 123, 127 (1955). Under the Atomic Energy Act of 1946, there was only one type of clearance possible for access to Restricted Data—the “Q” clearance.

\(^3^2\) The time estimates are taken from an address by Mr. Charles G. Manly, of the AEC’s Division of Civilian Application, before a meeting of the Committee on Atomic Energy Procurement of the Machinery & Applied Products Institute in Washington, D. C., July 27, 1955.

\(^3^3\) The AEC allows each firm twenty-five free security clearances and will bill the firm $15 for each additional “L” clearance requested and $265 for each additional “Q” clearance requested. Ibid.


\(^3^5\) Id. §25.1.
mencement of such activities. On the second level, Secret Restricted Data will be
made available on a narrow basis only, and only to an applicant who can demonstrate
that specific and limited Secret information has an "immediate or significant effect"
on his business, trade, or profession.\(^{36}\) In this respect, the AEC seems to be estab-
lishing a new form of "need to know"—"need to know" to carry on private activi-
ties for profit.\(^{37}\)

Confidential and Secret access permits have a number of features in common. Under both types of permits, actual access is limited to persons with appropriate se-
curity clearance—"L" clearance in the case of Confidential access and "Q" clearance
in the case of Secret access;\(^{38}\) the applicant must agree in writing to conform to all
AEC security regulations\(^{39}\) and must submit proposed procedures for safeguarding
the Restricted Data for AEC approval;\(^{40}\) and those given access will be required to
reimburse the Commission for readily identifiable cost of services rendered by the
Commission in connection with the agreement, including the costs of clearance and
of publications or documents furnished.\(^{41}\) There is one significant difference, how-
ever. In the case of Confidential access permits, the Commission does not reserve
any rights to inventions and discoveries arising from the access, while in the case of
Secret access permits, the Commission retains the right to use inventions or dis-
coveries arising from the access on a royalty-free, non-exclusive basis.\(^{42}\)

Those holding Confidential or Secret access permits may obtain access to Re-
stricted Data within the scope of their permits from private persons as well as from
the AEC directly. As the Director of the AEC's Division of Civilian Application
put it:\(^{43}\)

after the personnel security clearances have been obtained, the permittee may obtain the
restricted data for which he has been given a permit anywhere he can find it—AEC con-
tractors, other AEC permittees, and Commission offices.

Any person possessing Confidential Restricted Data pertaining to civilian applica-
tions of atomic energy may permit any individual in his own company or elsewhere
who has an "L" or a "Q" clearance to have access to such information.\(^{44}\) Secret
Restricted Data may be made available to any individual within his company who
requires access in the performance of his duties.\(^{45}\) But Secret Restricted Data may

\(^{36}\) Id. \(\S\)25.8(a)(2).
\(^{37}\) Charles G. Manly, of the AEC's Division of Civilian Application, stated in an address before the
Atomic Industrial Forum in San Francisco on April 4, 1955: "... the Atomic Energy Commission
now accepts a purely commercial interest... as sufficient 'need to know' to warrant access to Confi-
dential Restricted Data."
\(^{39}\) Id. \$25.9(c)(1).
\(^{40}\) Id. \$25.11(b).
\(^{41}\) Id. \$25.9(c)(2); see note 33 supra.
\(^{43}\) Address of Harold L. Price, Director of AEC's Division of Civilian Application, before the Atomic
\(^{44}\) Proposed AEC Regulations for the Safeguarding of Restricted Data \$95.31, 20 Fed. Reg. 2495-96
(1955).
\(^{45}\) Ibid.
not be made available to any other individuals except as specifically authorized by the AEC. This means that whenever an inter-firm exchange of Secret Restricted Data is contemplated, the parties must communicate with the AEC for permission to exchange the information.

The AEC’s public statements and its proposed regulations issued to date set forth only the bare outlines of the regulatory scheme within which the classified atomic energy technology will be made available to American enterprise. They avoid, it would seem almost deliberately, the many serious and vexing problems inherent in the effort to mesh security control over technological information with use of information so controlled for private purposes. The information control mechanism forged in the Atomic Energy Act of 1954 and the opening of the atomic energy technology to private enterprise add a new dimension to the problem of effective security and compel serious thought about the impact of security upon the economy.

II

Some Problems Raised

Some major problems become apparent as we move forward into the era of a private atomic technology which will be based, to a large extent, upon private use of national secrets. What follows cannot be a complete discussion of the total implications of the information control structure, since each problem which is stated suggests a host of subsidiary or ancillary problems. These problems, moreover, are necessarily discussed in abstract terms, on the basis of the limited official statements and proposed regulations issued to date. In any event, time and actual experience in implementing the information control system will undoubtedly bring to light additional major problems and add an important gloss to the problems discussed in this paper.

The Scope of Access Which Will Be Permitted Under Access Permits

Under normal circumstances, any firm has available to it all the information necessary for it to compete effectively, assuming it has adequate personnel and resources, in the race for new or improved products or techniques. The only impediment to development and exploitation of new ideas rests in the patent system. In the new atomic energy industry, however, technological information is not readily available to all those who are willing to dig for it, but is, to a very significant extent, available only subject to the dispensation of the Government. The Government has, therefore, a great responsibility to assure that the atomic energy information control system is administered in an equitable manner which will discriminate neither in favor of nor to the detriment of individual firms.

The problem of assuring equitable dissemination of Restricted Data is greatly complicated by the present structure of the atomic energy industry—a structure which undoubtedly will persist into the foreseeable future. A number of firms have

\[46\] Ibid.
had substantial and comprehensive access to Restricted Data for many years in their roles as government contractors or under AEC study arrangements and have large pools of personnel who have acquired substantial classified know-how. At the other extreme, many firms aspiring to a role in the coming atomic era have had very little or no access to Restricted Data. Even among the former group, there are marked variations in the degree of classified know-how possessed, depending upon length of participation in atomic energy programs, scale of activities, and degree of diversification of the projects in which involved. Indeed, many of these firms undoubtedly already possess sufficient classified know-how to proceed with profit-seeking ventures in the atomic energy field without dependence upon the AEC for further access to Restricted Data. Competition for atomic energy profits is, therefore, commencing under circumstances involving substantial inequities in access to the classified technology. This situation appears to be an unavoidable consequence of the decision to open the atomic energy field to private enterprise. The competitive inequities are somewhat mitigated by the provisions of the Atomic Energy Act of 1954 intended to preclude the development of a patent monopoly during the transitional period, but even without the ability to secure a monopolistic patent position, the “haves” possess the opportunity to outstrip the “have-nots” in developing markets for atomic energy applications. Moreover, similar and additional advantages will continue to accrue in the future to those firms which participate under contract in the various programs conducted by the AEC. They will receive access to Restricted Data as an incident to their work for the AEC, for which, of course, they are compensated, and some of this information may be of the type which will not be available to other firms under access permits.

The AEC’s approach to information control does not reflect consideration of the problem of these initial inequities, which, in any event, may be insoluble. Rather, the AEC appears to accept the status quo and concentrates its attention upon assuring future equality of access among the “have-nots,” without regard to the advantages already possessed by the “haves.” But even this policy involves impediments to the ultimate redressing of the inequities.

Sections 152 and 159 of the Atomic Energy Act of 1954, 68 Stat. 944, 948, 42 U.S.C.A. §§2182, 2189 (Supp. 1954), bar the issuance of patents for atomic energy inventions made or conceived under any “contract, subcontract, arrangement, or other relationship with the Commission” or during the course of any federally financed operations, unless the AEC waives its rights to such patents. Section 153, 68 Stat. 945, 42 U.S.C.A. §2183 (Supp. 1954), provides for compulsory licensing of important privately owned atomic energy patents under certain specified circumstances as the AEC deems appropriate under the statutory standards. The compulsory licensing provisions apply to patent applications filed during a transitional period ending September 1, 1959, by which date, presumably, the initial advantages of the “haves” will be greatly diminished.

There is no effective means for compartmentalizing and separating Restricted Data acquired by a firm through AEC contract activities from Restricted Data acquired by it under an access permit. Nothing precludes a firm’s use of Restricted Data, acquired by it in performance of an AEC contract, in connection with private exploitation of civilian applications of atomic energy under an AEC license. Indeed, there are undoubtedly many firms which can acquire in their contract activities all the Restricted Data which they possibly would require for effective conduct of AEC-licensed activities, so that they would never need an access permit as the basis for obtaining Restricted Data necessary for exploitation of civilian applications of atomic energy.
The AEC's proposed regulations contain three major restrictions upon the scope of Restricted Data to which access will be afforded under the Access Permit Program. Access to Restricted Data will be permitted only if it relates to civilian uses of atomic energy and is not "primarily of military significance";\(^4\) Secret Restricted Data will be made available only on an extremely limited basis and only to those who the AEC decides "really need it";\(^5\) and Top Secret Restricted Data is wholly excluded from the scope of access permits. These limitations, if they are to be regarded as effective, appear at first glance to be thoroughly reasonable, but they are, in fact, discriminatory. As will be pointed out, however, there is serious question whether these limitations can really be enforced by the AEC, and, if they are not enforceable, the discriminations discussed in the following paragraphs may not, in fact, be as serious as they would otherwise appear.

The line between civilian and military applications is, at best, a hazy one. Many areas of information which are, at any point of time, of primarily military significance also have substantial civilian application,\(^6\) and as time goes on, the relative degree of civilian significance is likely to increase. If, for example, the AEC chooses to regard Restricted Data relating to nuclear propulsion as "primarily of military significance" because of its present importance to military aircraft and naval vessels,\(^7\) the practical effect will be to exclude entry into these fields by additional firms interested in private research on and development of nuclear propulsion. It will also strengthen the competitive position of the firms now working in these fields under government contracts in connection with the ultimate development and sale of nuclear propulsion units for civilian application in locomotives, merchant vessels, motor vehicles, and aircraft. Similarly, the exclusion of Top Secret Restricted Data from dissemination to access permittees precludes some firms from working with important technological information—usually of the most advanced nature—while other firms have access to the same data as AEC contractors and are able, as a practical matter, to use the data in the competitive race for civilian markets.\(^8\)

\(^5\) It is clear that dissemination of Secret Restricted Data will be stringently limited. The AEC regards Secret Restricted Data as "particularly sensitive" and "will not permit it to be disseminated except to individuals who really need it." Address of Harold L. Price, supra note 43. The AEC has also indicated that access to Secret Restricted Data will always be limited "to only a few." Address of Charles G. Manly, supra note 37. A further indication of the AEC's attitude with respect to Secret access permits may be sensed in considering the statement that: "... a company usually has trouble showing that secret data will have an immediate or significant effect on their business until they have exhausted the confidential information available." Address of Charles G. Manly, supra note 32.

\(^6\) A leading authority on the content of Restricted Data, the former AEC Director of Classification, has stated: "I know of techniques important to atomic weapons manufacture and therefore highly classified which some clever individual might be able to turn to commercial use." Beckerley, supra note 31, at 126.

\(^7\) In this connection, it is noteworthy that certain bilateral agreements for cooperation with other nations in atomic energy matters entered into by the AEC specify that "the development of submarine, ship, aircraft, and certain package power reactors is presently concerned primarily with their military uses," and, therefore, beyond the scope of the agreements providing for exchange of information on civilian applications. See texts of Proposed Agreements for Cooperation Concerning the Civil Uses of Atomic Energy between the United States and Belgium, the United States and the United Kingdom of Great Britain and Northern Ireland, the United States and Canada, S. Rep. No. 1951, 84th Cong., 1st Sess. 18 (1955).

\(^8\) See note 48 supra.
Much the same analysis applies to dissemination of Secret Restricted Data. The AEC will undoubtedly exert pressure to persuade applicants for Secret access that they should try to find their information in the Confidential literature.\textsuperscript{64} If a Secret access permit is issued, it will authorize access within one or more specifically requested categories of Restricted Data to be established by the AEC. As a practical matter, however, a particular firm may not grasp the significance or relationship to its project of certain areas of Secret information, which it may not even know exists, while other firms may already have the Secret information or knowledge of its existence through work as AEC contractors or through acquisition of personnel who have been engaged in such work. Similarly, a firm may request access to a specific area of Secret data and be denied access on the basis of a bureaucratic determination that it does not really need such information, while an identically situated firm may be more successful.

A variation of the same problem may be found with respect to access to Confidential Restricted Data. The AEC has indicated that it is reviewing various reports and documents in the field of civilian applications and that these materials will be listed in a catalogue, printed, and made available for sale to permittees.\textsuperscript{56} But the AEC cannot hope to include in such reports all extant Restricted Data on civilian applications.\textsuperscript{65} This means that some firms which have been in the atomic energy program for a time will have available pieces of Confidential Restricted Data that would not be available to other firms through the use of the AEC's catalogue and published reports. Such other firms may or may not be able to obtain such unpublished Confidential Restricted Data, depending upon their luck in finding people who happen to have the data and who are willing to make it available.

Sound and conscientious administration of the Access Permit Program would undoubtedly narrow the area and frequency of discrimination and inequality. Indeed, it must be recognized that it is rarely possible for a sovereign to treat identically situated persons in a precisely identical manner. There are, inevitably, variations leading to some degree of discrimination, usually an insignificant degree if administration is sound. But we are dealing here with technological information, which in a normal economic situation is freely available to access. Government-imposed restraints upon the flow of information are, in essence, abhorrent. Total restrictions upon access to information have been tolerated in the interests of national security, but restraints unevenly applied as among competing firms are another matter. Access to Restricted Data is the immediate gateway to the atomic future of American industry. The slightest deviations in equality of access to Restricted Data may be of the most profound immediate and long-run significance to the economic status of the

\textsuperscript{64} See note 50 supra.
\textsuperscript{65} Address of Charles G. Manly, supra note 32.
\textsuperscript{66} The classified reports which will be made available by the AEC are largely "pin-point" research reports rather than generalized or comprehensive assessments of methods, approaches, and outlook. Permittees will have to "examine stacks of reports, here and there select and evaluate bits of information, and make their own analyses." \textit{Ibid}. 
firm affected, to the relative position of competing firms, and to the basic structure of our future atomic economy. The situation is rendered all the more serious by the fact that these deviations are created by the Government through application of vague and subjective standards.67

These problems are functions of the manner in which the 1954 act is administered rather than of deficiencies in the act itself. Congress did not blueprint the pattern for dissemination of Restricted Data for use by private enterprise, but merely established a set of contrary principles for security control and industrial dissemination, leaving the AEC virtually absolute flexibility in implementing these principles.

The AEC's approach to implementation of these contrary principles represents a peculiar blend of the considerations involved. In so far as concerns Confidential Restricted Data on civilian applications of atomic energy not primarily of military significance, there is an almost complete abandonment of the "need-to-know" concept. This minimizes the problems of discrimination in access but makes effective security control quite difficult. There is reason to believe that the AEC expects that Confidential Restricted Data disseminated so widely will be compromised and declassifiable within a relatively short time but regards continuation of information control during this marginal period as important.68 Secret Restricted Data, however, is disseminated only on a fairly stringent "need-to-know" basis, although purely commercial "need to know" is recognized. Top Secret data is disseminated only on an absolute "need-to-know" basis and is not made available for commercial use. Thus, there is a serious effort to maintain genuine security and a corresponding increase in the inherent potential discrimination.

It is readily apparent that the traditional concept of free competition requires free entry to the market place. The necessity for effective security cannot be reconciled with this traditional concept. The attempt to maintain effective security and, at the same time, spur private development and exploitation of atomic energy inevitably gives rise to serious questions of political and economic policy and of justice, and these questions are particularly troublesome because of their impact upon the basic structure of what will be a basic and important American industry.

The Restricted Data Fantasy

In some important respects, the AEC's approach to information control reflects a lack of realism bordering upon fantasy. Nowhere is this lack of realism more

67 The AEC's proposed regulations do not contemplate that there will be "due process" in the AEC's handling of access permit applications and related questions. The act expressly provides for hearings and judicial review only in connection with proceedings for the granting, suspending, revoking, or amending of any license. § 189, 68 Stat. 955, 42 U.S.C.A. § 2239 (Supp. 1954). Although the act does not in any sense mention access permits, however, it is clear that an access permit is the equivalent of an atomic energy license, and, in many respects, access permits may be of greater economic importance than licenses expressly provided for in the act. Nevertheless, the Proposed AEC Regulations on Rules of Practice, 20 Fed. Reg. 5786 (1955), provide for hearing procedures only with respect to licenses expressly referred to in the act.

68 Continuation of information controls gives the AEC a valuable bargaining asset in connection with negotiation of bilateral agreements for cooperation with other nations.
apparent than in the AEC's apparent assumptions about the creation and circulation of Restricted Data.

Implicit in the proposed information control regulations are the assumptions that Restricted Data can be neatly packaged and dispensed; that persons may lawfully possess Restricted Data only if authorized by the AEC; that dissemination of Restricted Data may be confined within AEC-controlled channels; and that lawful access to Restricted Data may be terminated when the authorization for access expires. These assumptions all collapse when it is recognized that the creative mind of man is able, independently and without AEC assistance, to originate and develop information falling within the Restricted Data definition. A firm which has never had an AEC contract or an access permit and none of whose personnel has ever had access to Restricted Data may, nevertheless, create information falling within the Restricted Data category. Similarly, a firm which has an access permit and is, therefore, authorized to have access to some Restricted Data may originate Restricted Data of a type beyond the scope of the permit's authorization. Thus, a permittee may originate Restricted Data of a type which he is not authorized to possess because it is primarily of military significance, or Top Secret Restricted Data, or Secret Restricted Data not authorized under the access permit.

An AEC license is not required to originate new ideas in the atomic energy field. No law or regulation is violated if a firm develops Restricted Data notwithstanding that it does not have an access permit authorizing access to the data created. But once the Restricted Data comes into existence, it becomes subject to the entire array of information control provisions of the Atomic Energy Act of 1954 to precisely the same extent as if the data had been developed in an AEC laboratory. A firm

69 In the recent Hearings, supra note 23, Senator Humphrey, Chairman of the Subcommittee, questioned the AEC's General Counsel, Mr. William Mitchell, about the situation which would arise if a scientist independently developed and wished to publish energy information falling within the Restricted Data definition. The following colloquy ensued (at 268-70):

Mr. MITCHELL. I am assuming that this scientist knows that the information that he has developed and is publishing falls within the category of restricted data. . . . I think when this came to our knowledge, we would immediately call to his attention the fact that this information does fall within this area, and we would call to his attention the need for safeguarding it, and not passing it on to people who are not entitled to receive it.

Senator HUMPHREY. If he were going to continue his investigation, he would have to be cleared?

Mr. MITCHELL. I think he would.

Senator HUMPHREY. What about his publishing these ideas?

Mr. MITCHELL. Well . . . I would say that at this point, he is on notice, that the kind of thing he is doing not only the information he already has developed but the information that he may continue to develop falls within this area. Then I think he is on notice that if he passes this new information on to people who are not entitled to receive it, I would think that this would be a knowing revelation.

Senator HUMPHREY. . . . Let us assume . . . that he cannot get a security clearance. That he joined something that he should not have joined. He does not get a security clearance. So you cannot hire him. You cannot have anything to do with him. What do you do with this fellow? He is a scientist. He has a laboratory. He likes to work in his laboratory. He researches and he produces and he publishes. What do you do with him in America?
which originates such Restricted Data, even if it was developed wholly without government assistance or connection, must then become concerned with classification stamps, investigations, clearances, safe, and other trappings of security, and severe security restrictions are placed upon the flow of the firm's ideas. The firm finds itself propelled, involuntarily, into a security vortex of considerable economic significance.

The fact that Restricted Data may be independently originated demonstrates clearly that the AEC has no real power to deny or control access to Restricted Data. If, for example, it refuses to grant an access permit for certain Secret Restricted Data on the grounds that the data does not have an immediate or significant effect upon the applicant's business and that the data is primarily of military significance, the applicant may completely circumvent the AEC's refusal by developing the very same information itself without obtaining the data from the AEC or from other firms which have the information. Indeed, it can do this speedily and effectively simply by hiring away from other firms personnel skilled in the particular classified technology. Such personnel could not bring classified materials with them, and they would lose their AEC clearances when they changed jobs. They would, moreover, be precluded from discussing Restricted Data with or communicating Restricted Data to the officials and other employees of their new firm unless such officials and employees had clearance and authorization for such access. But there is nothing to prevent or prohibit their using their minds' store of Restricted Data to develop atomic energy plans and ideas. It is not conceivable that the AEC could find statutory authority or would find it wise as a matter of policy to refuse to clear officials and other employees of the firm and authorize them to have access to Restricted Data developed by the firm's own personnel at its own expense so that the firm could have the benefit of this work.

Thus, a firm denied access to Restricted Data may easily present the AEC with the fait accompli of having achieved its purposes legally without AEC authorization. It would have a body of Restricted Data available to it and a pool of cleared personnel to work with the data. The AEC would then have no sound basis for refusing to permit the firm to discuss this type of information with other firms.

Mr. MITCHELL. So far as I know, we have never run into this situation. If we did, I would say that if this man is on notice that the things that he is doing have an important impact on our national defense and security, and if he chooses in spite of this knowledge, to pass this information on, to people who are not entitled to receive it, then he quietly [sic] properly becomes subject to the criminal provisions of the law. . . .

Senator HUMPHREY. In other words, you could really put him in jail?

Mr. MITCHELL. I think we could.

Mr. MITCHELL. That is right.

Senator HUMPHREY. But you could force him to shut up?

Mr. MITCHELL. Yes, sir.
working in the field or for refusing to permit access to pertinent Restricted Data directly from the AEC. In other words, the circumstances would, in all probability, compel the AEC to grant the very access permit which it had previously denied. If it does this, there would be no basis for refusing to grant similar access permits to other applicants who are in a situation similar to the initial one of the firm which circumvented the restrictions.

A related problem is that of the limited term of access permits. Under the proposed access regulations, access permits will generally be issued for a period of one year, subject to renewal, and Secret access permits may be issued for even shorter periods. During the period of the permit, the permittee will be able to obtain Restricted Data from the AEC and from other firms and to purchase numerous classified documents. The permittee will, presumably, also create numerous internal documents reflecting or extending the classified information acquired from external sources. What happens to this store of Restricted Data if the access permit expires and the permittee does not seek renewal?

The AEC's proposed regulations do not indicate how the security interest in a firm whose access permit terminates will be liquidated in the face of the permittee's acquisition of a substantial proprietary interest in Restricted Data. Although the AEC could conceivably require the return of all classified documents obtained from external sources, it is doubtful that it could compel surrender of the firm's original documents. There is, moreover, no way to purge the firm of its classified know-how stored in the minds of its personnel. Undoubtedly, the AEC will insist that its security regulations remain in effect, just as if the access permit were still in force, to protect the Restricted Data in the hands of the former permittee. Similarly, it is almost certain that all security clearances would remain in effect and that additional clearance requests by the firm would be processed by the AEC to avoid the anomaly of uncleared personnel having access to the firm's Restricted Data. On the other hand, if the clearances are permitted to remain in effect, it is unlikely that

---

60 Nothing in the Atomic Energy Act of 1954 precludes the issuance of a license for atomic energy activities based upon Restricted Data outside the scope of the Access Permit Program. Thus, a firm which develops or otherwise possesses Top Secret Restricted Data, or data of primarily military significance, which wishes to obtain a license for civilian applications based upon such data, may apply for a license and would be entitled to have its application considered on precisely the same basis as if it involved only Restricted Data to which access was authorized under the AEC access regulations.


62 It is not at all inconceivable that a permittee may conclude that it does not wish to renew its access permit if it can lawfully continue to work with Restricted Data without it, since it may regard the conditions attached to the permit as unduly onerous. A permittee must agree, for example, as a condition of the permit, to waive certain patent claims in connection with inventions or discoveries made or conceived in the course of, in connection with, or under the terms of the permit and to grant an irrevocable, royalty-free, non-exclusive license in and to report to the AEC any invention or discovery made or conceived as the result of access to Secret Restricted Data under the permit. Proposed AEC Regulations on Access to Restricted Data §25.9(c), 20 Fed. Reg. 3634 (1955).

63 See Proposed AEC Regulations on Safeguarding of Restricted Data §95.2, 20 Fed. Reg. 2495 (1955). This is applicable to all persons within or under the jurisdiction of the United States, and not merely to persons possessing Restricted Data under some form of AEC authorization.
the AEC could prevent cleared personnel of the firm from discussing Restricted Data with other firms, thereby expanding its store of classified know-how.

It is difficult to understand how termination of an access permit can substantially affect a firm's position with respect to Restricted Data. It would appear that once a firm achieves the status of having authorized access to Restricted Data, its status cannot be easily undone. It remains to be seen whether the AEC will find a realistic formula for distinguishing between those firms which continue to renew and those firms which choose to abandon their permits. This is, in a sense, the acid test of the efficacy of the AEC information control mechanism, since if a firm can retain many of the advantages of an access permit even though it renounces its permit, the entire Access Permit Program becomes almost an absurdity.

The Problem of Clearance

The AEC's access program provides a means for controlling the dissemination of Restricted Data to individuals with appropriate security clearance. A further control is exercised by the AEC in determining who is to be cleared. The access program operates directly upon the firm, and only indirectly upon the individual employee; the clearance program operates directly on the employee, and only indirectly upon the firm. But the impact of the clearance program upon the relative position of competing firms is by no means insignificant. A clearance problem may seriously retard or prevent entry of a firm into classified areas of the atomic energy industry or may adversely affect its competitive position within the industry, especially where it is a small firm or where an uncleasurable employee is essential to the firm's atomic energy activities. As a corollary of this, possession of AEC clearance or a pool of cleared personnel is a most valuable asset in that it greatly expands the economic potential of both the cleared individuals and the firm. Possession of clearance means that one can act to take immediate advantage of classified opportunities. An individual or firm without clearance cannot always move to capitalize on such opportunities. The most that can be done in many cases is to mark time while a clearance application is being processed, during which interval competitors who already have clearance status are actively engaged in taking advantage of the opportunity.

Two distinct steps are involved in the clearance process. The first step is the AEC's decision to process an application for clearance. The second step is the determination that clearance should be granted in the light of the results of investigation. Both of these steps involve considerations of the utmost importance to private enterprise engaged in atomic energy activities.

The Government has never been generous in dispensing security clearance. Under traditional security practices, the principle of "need to know" has been applied mainly in the initial granting of clearance rather than in the actual dissemination of classified information. There was no such thing as a "general" security clearance authorizing access to classified information generally. Clearance applications were
never processed just because an individual wanted a clearance in case he might need it or because it would help in getting classified work. Clearance applications were usually entertained only when someone already within the circle of cleared persons engaged in work for the Government would request clearance of an individual so that he might participate in a specific classified government project. Once the individual was initiated into the cleared circle, his clearance would, as a practical matter, enable him to have access, without further determination, to other classified matter than that for which the clearance was initially granted. As soon as the need for access to classified matter for performance of work on government projects ceased, the clearance was, theoretically at least, terminated.

This was precisely the pattern of the AEC clearance program in less complicated days when the AEC did not have to be concerned with making Restricted Data available for private exploitation. Under present conditions, however, the rules are quite different. The Commission will now process for “L” clearance almost any individual who can show that there is a potential use for Restricted Data in his business, profession, or trade. After “L” clearance is granted, it suffices for access to any Confidential Restricted Data without regard for the “need-to-know” principle.

The requirements for “Q” clearance are more severe. “Q” clearance may be granted to private persons for exploitation of Secret atomic energy technology only under an access permit. A Secret access permit will be granted only for specific areas or information having an immediate or significant effect upon the applicant’s business, profession, or trade and only for definitely limited periods of time. Thus, “Q” clearance for access to Secret Restricted Data is linked to a severe “need-to-know” test, although the “need to know” may now relate to private profit-seeking activities as well as to government projects. This means that firms which cannot show a “need to know”—i.e., that the information requested has an immediate or significant effect—will not be able to get a Secret access permit or a “Q” clearance. When a business opportunity does arise in which Secret Restricted Data would have an immediate or significant effect, the firm may apply for “Q” clearance for its personnel and expect to receive the clearances in three or four months if all goes well. Meanwhile, the opportunity may have been captured by someone with a clearance status which permitted immediate action.

This suggests the strong desirability of divorcing the processing of clearance applications from access permits and the “need-to-know” doctrine. It would make sense for the AEC to process for “Q” clearance anyone requesting it who could show that such clearance might be of potential value to him. The “need-to-know” principle could then be applied to actual access to Restricted Data rather than to the grant of clearance. For example, the “Q” clearance could be held in inactive suspense until a “need to know” arises, at which time, it could quickly be made active. Such a policy would be in no way inconsistent with principles of effective security; indeed, it would make for more effective security, since application of the “need-to-know” doctrine would be more realistic and efficient.
The second step in the clearance process is the determination whether the applicant is worthy of clearance. This determination is part and parcel of the over-all problem of government personnel security programs, which has been very much discussed in the past several years. But the atomic energy information control system carries the personnel security clearance concept into new ground, raising new questions of law and policy, since AEC security clearance is substantially equivalent to a license for employment in the atomic energy industry. The opportunity for private employment has long been recognized as a right subject to the protection of the “due process” clauses of the fourteenth and the fifth amendments to the Constitution of the United States. It is a certainty, because of the economic significance of AEC clearance, that the clearance requirements for access to Restricted Data by employees of private enterprise will, sooner or later, be subjected to court tests. It remains to be seen whether the courts will countenance, as they have in the cases of government employees, disposition of important rights to private employment under the vague standards and loose procedures, falling far short of “due process,” which are characteristic of the present-day security clearance systems. Judicial rejection of the AEC clearance system as applied to employees of private enterprise engaged in private exploitation of atomic energy applications would throw the entire information control system into absolute chaos.

III

Conclusion

The above discussion clearly demonstrates the difficulties found in rational application of security controls to areas of economic activity entrusted to the play of private enterprise. Problems of information control were relatively simple when they arose only in the context of government operations and programs, where the Government’s control was absolute and it did not have to be overly concerned about

---

64 Theoretically, security clearance is required only for access to Restricted Data and not for employment in the atomic energy industry. Denial of clearance means only that the individual may not have access; it does not mean that the employer must remove him from unclassified atomic energy work. As a practical matter, however, an unclearable employee is a handicap to his employer, since the employer is deprived of flexibility in the assignment of the employee to areas of work and the employer must take extraordinary pains to keep a security risk away from any possible area of security interest. In addition, an employer interested in classified atomic energy activities might understandably be reluctant to retain an employee who is persona non grata with the AEC for security reasons. At the very best, denial of AEC security clearance would greatly diminish an individual’s economic opportunity in atomic energy.

65 See Meyer v. Nebraska, 262 U.S. 390 (1923); Cummings v. Missouri, 71 U.S. 277 (1867); United States v. Gray, 207 F.2d 237 (9th Cir. 1953); Parker v. Lester, 112 F. Supp. 433 (N.D. Cal. 1953).

66 In the cases of government employees, the theory that no person has a right to a government job has been decisive, since if there is no “right,” there is no deprivation to which the “due process” requirement attaches. It has, however, been recognized that deprivation of the right to private employment in the merchant marine under the Government’s port security program (which is analogous to the personal security programs) must be accomplished in accordance with “due process.” On October 26, 1955, the United States Court of Appeals for the Ninth Circuit held in Parker v. Lester, reversing Parker v. Lester, supra note 65, that a merchant seaman must be afforded the elements of due process, including the opportunity to confront and cross-examine those furnishing derogatory information against him, before he may be denied employment on security grounds. See 24 U. S. L. WEEK 2203-04 (U. S. Nov. 8, 1955).
equity, discrimination, due process, and the effect upon competitive forces. Application of security principles developed in this context has now been uncritically transferred to the sphere of competitive free enterprise. It has been assumed that the standard principles hitherto applied can be carried over almost intact, and with only minor tinkering, to this new sphere. This assumption has been clearly articulated by the AEC.

The proposed regulation dealing with the safeguarding of Restricted Data is pretty much an adaptation of information control procedures which have been in effect within the Commission program since its beginning....

There is considerable question whether simple adaptations of conventional information control procedures can adequately meet the needs of either private enterprise or security.

The AEC's approach to information control in atomic energy development assumes that access to Restricted Data will be granted by a paternalistic government which, with due regard to the requirements of national security, industrial progress, and principles of equity, will make fine distinctions among competing firms and types of information. The impersonal objectivity of the market place would be replaced by the whimsical subjectivity of a bureaucracy riding the horns of an insoluble dilemma in governing access to the atomic energy industry. If the AEC's proposed regulations embodying this structure of information control are to be taken seriously, there can be no result other than the lessening of competition, the encouragement of monopoly, the introduction of rigidities into the economy, and serious discrimination against those firms which, for one reason or another, cannot meet the bureaucratic tests. If the information control structure is, in fact, what it purports to be, one can only hope that sound and conscientious administration by the AEC will lessen the intensity and extent of these evils.

But, as pointed out above, it is possible that the basic discriminatory restrictions upon private enterprise's access to Restricted Data may be lawfully circumvented almost at will. If this is true, the evils inherent in the information control structure are drastically reduced, in the long run at least, since any firm which really wants access to Restricted Data and has the requisite ingenuity and resources can accomplish its objective despite the restrictions. But it remains a serious problem that the discriminatory restrictions on access will be effective in the short run—during the formative infancy of the atomic energy industry—until the pattern for circumvention has been demonstrated and accepted.

There is another important problem presented by the contemplated structure of information control. This is the problem of preserving the integrity of the AEC security mechanism itself. The integrity of the security mechanism is considerably

67 In the context of conventional security programs, the only problems of equity and discrimination center upon selection of particular firms for work on classified government projects, and there is little direct impact upon nongovernment activities.

68 Address of Charles G. Manly, supra note 32.
weakened by abandonment of the "need-to-know" criterion with respect to Confidential Restricted Data and its attenuation with respect to Secret Restricted Data. It is, moreover, doubtful that the AEC can hold the line established in its proposed regulations. Whenever an applicant for Restricted Data is denied access as required by the regulations, the applicant would undoubtedly be justified in raising the cry of "discrimination" since it will never be difficult to find another firm which is using the same Restricted Data. It cannot be expected that a government agency will not yield in the face of such pressures. Beyond this, if it is a correct hypothesis that restrictions upon access to Restricted Data may be easily circumvented, it is most doubtful that the AEC will ever be able to deny access to any type or classification of Restricted Data to any applicant who really wants it, except possibly to applicants who cannot meet the security clearance tests. Never before has the security mechanism encountered persistent, erosive resistance such as it will now face as competitive enterprise seeks to exploit every crack and crevice in the security armor to avoid and evade restrictions barring the path to profit-seeking activities. This presages a complete collapse of the security mechanism.

The AEC has rushed headlong into the new experiment in information control without full and adequate consideration of its implications. A problem of this magnitude and novelty, involving not only questions of economic and legal policy and effective security, but also problems of essential freedoms of man, should not be entrusted to the discretion of the government agency whose gropings for a reasonable solution lead inevitably to questionable decisions which may not be easily rectified in the light of hindsight. The dilemma of information control—the reconciliation of the needs of national security with the desire to encourage industrial development of atomic energy—should, instead, be resolved as a matter of considered national policy after full study of all issues involved.