Chapter 5

The 1980s: Converging Restrictions on Scientific Communications

CONTRACTUAL RESTRICTIONS ON COMMUNICATIONS

Most universities are reluctant to undertake classified research, but many are willing to accept contractual restrictions that have the same effects.

Dissemination of scientific information or technical data[1] can be and often is restricted by the terms of written agreements between government funding agencies and nongovernment researchers. Most universities are reluctant to undertake classified research, but many are willing to accept contractual restrictions that have the same effects. In some cases, indeed, refusal to accept such contracts is considered by faculty to be an infringement on their academic freedom. Some civil Libertarians, on the other hand, object to such contracts. While a contract, freely entered into, is assumed to benefit both parties to it, this does not provide for consideration of the public interest (and investment) in scientific knowledge, which may not entirely coincide with or be limited to national security interests.

The government often requires that contractors and grantees agree to submit publications resulting from nonclassified government-sponsored research for prepublication review. This raises the question of prior restraint. There are, however, no reported court decisions involving prepublication review clauses in contracts and grants to universities.

National Security Decision Directive 84 (NSDD 84),[2] issued on March 11,1983, requires all present and future government employees to sign a lifetime nondisclosure agreement as a condition for access to classified information, or to "Sensitive Compartmented Information" (SCI). Federal classifying agencies have the right of pre-review of public statements, lectures, and speeches. Contacts between media representatives and agency personnel are controlled. This directive was aimed primarily at Federal employees, but secrecy agreements can also be required of government contract researchers under the directive.[3]

According to a recent study supported by the Fund for Investigative Journalism, by the end of 1985 more than 290,000 individuals had signed lifetime prepublication review agreements (Non-disclosure Agreements Standard Forms 189 and 189A) under NSDD 84, and more than 14,000 speeches and articles had been submitted for review.[4] There have been strong protests against the requirement for lifetime agreements. However, the Federal Government takes the position that the contractual obligation of an employee overrides First Amendment protections.

In *Snepp v. United States*[5] the Supreme Court found no constitutional impediment to enforcing such an agreement. This case, however, involved CIA employees, and the intelli-

[1] As already noted, national security officials tend to make a sharp distinction between "scientific" communications and technical, technological exchanges that is not always either clear or acceptable to researchers in an area.

[2] The nature of National Security Decision Directives is discussed below.

[3] Secrecy agreements or contracts used within the intelligence community were found to be a proper enforcement device in 1980 by the Supreme Court *(Snepp v. U. S.,* 444 U.S. 54)

[4] Donna DeMoc, "Sworn to Silence, " The Progressive, May 1987, p. 29. The study presumably covered SF 189s: SF 189A was approved for inclusion in the Industrial Security Manual in late April 1987.

[5] 444 **Us. 507 (1980).**

gence community is generally conceded to have particularly strong interests in internal security. Two Circuit Court decisions, one before and one after Snepp,[6] indicate that such an agreement might not be enforceable if classified information is not involved. These cases did not involve research results or scientific information.

NSDD 84 also sought to expand the use of "lie detectors" by Federal agencies. Executive branch employees can be required to submit to polygraph examinations for access to certain classified information, or in the course of investigations of unauthorized disclosure of classified materials. The threatened expansion of polygraph use brought strong protests. In the fall of 1983, Congress temporarily prohibited implementation of the polygraph provision, and President Reagan agreed not to pursue this policy immediately.[7] In effect, the provisions of NSDD 84 dealing with polygraphs have been rescinded, except as they pertain to DoD, where polygraph tests are widely used not only in investigations but for routine screening of recruits, promotions, etc.

[6]The first was United States v. *Marchetti*, 366 F.2d 1309 (4th Cir., 1972). *cert. den.*, 409 U.S. 1063 (1972). The second was *McGehee v.* Casey, 718 F.2d 1137 (D.C. Cir., 1983).

[7]Harold C. Relyea, *National Security Controls and Scientific Information*, Congressional Research Service Issue Brief B82083, updated June 17, 1986, p. 69. See also National Academy of Sciences, Committee on Science, Engineering, and Public Policy, Panel on Scientific Communication and National Security, *Scientific Communication and National Security*, 1982.

RESTRICTIONS ON INFORMAL COMMUNICATIONS

Classification, legislative mandates, contract agreements, and export controls have all been used in the last decade to restrict *informal* communications among scientists.

Classification, legislative mandates, contract agreements, and export controls have all been used in the last decade to restrict informal communications among scientists. By informal communications is meant modes of communication other than formal publishing: speaking, classroom teaching, participation in professional meetings and seminars, and similar activities. Restrictions on campus teaching are particularly irksome to many scientists. Since the 1970s, there has been a steady influx of foreign students to U.S. universities. Any restrictions on who may be taught what in a university are of profound importance, infringing on academic freedom, on institutional responsibility, and on the prestige and economic viability of the institution.

In 1980, the Department of State informed Cornell University that a visiting Hungarian engineer would have to be limited to classroom pursuits and could not participate in certain professional seminars or receive prepublication copies of research papers. Rather than abide by these restrictions, the university canceled his visit. Later that year, the Department of State, acting under export restrictions, asked universities to prohibit visiting Chinese students from engaging in certain studies.[8] There were reports of a few instances in which universities, in ill-considered, hasty responses, listed short courses or seminars "for U.S. citizens only;" such decisions were apparently few, and were soon terminated.[9]

On February 27, 1981, the presidents of five leading universities (Stanford, the California Institute of Technology, the Massachusetts Institute of Technology, Cornell, and the Univer-

[8]Relyea, op. cit., p. 4.

[9]There were references in the press at that time to university courses or seminars so advertised, but recent discussions with a number of education association officials identified only one specific incident of a course listed "for U.S. citizens' at a university, and that decision was said to have been quickly overruled.

Scientific exchange is a primary purpose and role of professional societies.

sity of California) sent a letter of protest to the Secretaries of Commerce, State, and Defense. The university presidents said that the government had resorted to measures that could "irreparably harm university-based research."[10]

Scientific exchange is a primary purpose and role of professional societies. These organizations depend on their members to judge whether communication of research results or other information violates national security restrictions, and they can be faced with dilemmas when their members either intentionally or inadvertently transgress. In February 1980 there were strong efforts by the Carter Administration to regulate the communication of scientific information by professional societies. When the American Vacuum Society organized an international meeting on magnetic bubble memory devices, the Department of Commerce notified the society that the expected presence of nationals of certain foreign countries subjected the proceedings to compliance with export licensing. The Association promptly rescinded invitations to scientists from Hungary, Poland, and the U.S.S.R. Chinese scientists, already en route, were allowed to attend after signing an agreement not to "re-export" to nationals from 19 countries what they learned. [11]

In August 1982, 4 days before a meeting of the Society of Photo-Optical Instrumentation Engineers (S PIE), DoD learned that four Soviet scientists were to attend. DoD confiscated of dozen papers from DoD employees who were to present them at the meeting, and notified

Under current DoD directives, unclassified papers containing export-controlled information cannot be presented at professional and academic meetings unless dissemination and access controls are "equivalent to those used for distributing the data directly by DoD."

the organizers that other papers were sensitive. DoD representatives were present as the meeting began and questioned participants as to whether their papers resulted from work sponsored by DoD and whether they had received clearance. One hundred papers were withdrawn. A SPIE official later said that government officials had overreacted to the presence of Soviet citizens, and that SPIE members themselves had probably panicked at the sudden crackdown. Many of the papers that had been hurriedly withdrawn were later cleared and published or presented, although others were found to deal with classified research. [12]

Under current DoD directives, unclassified papers containing export-controlled information cannot be presented at professional and academic meetings unless dissemination and access controls are "equivalent to those used for distributing the data directly by DoD"[13]--so-called unclassified/limited access presentations.[14] This rule was applied on an ad hoc basis during another meeting of the Society for Photo-Optical Instrumentation Engineers in April 1985. Two weeks before the meeting, organizers were notified by DoD that a special session, organized by one of its members at a military base, with 43 papers scheduled,

[10] "(; finaBara Kolata, "Attempts To Safeguard Technology Draw Fire," *Science*, vol. 212, No. 4494, May 1981, p. 523. The letter also said: "There is no easy separation in any engineering curriculum. Furthermore, producing graduates with no hands on' experience in these areas would he of little value to American high technology industries.

[11] Ibid., p. 3.

[12] This account is based on discussion with SPIE director Joseph Yaver in May 1987; for a contemporary account, see Joel Greenberg, "Science's New Cold War," Science *News*, vol. 123, Apr. 2, 1983, p. 218. Also see Relyea, op. cit., 1986.

[13] "Statement supplied for (3TA by DoD officials, office of the Secretary of Defense.

[14] US Department of Defense, C) ffice of the Under Secretary of Defense for Research and Engineering, "Policy and Guidelines for the Presentation of DoD Sponsored Scientific and Technical Papers," draft proposal. Oct. 24, 19H5.

would have to be canceled because the papers could not be given in open sessions. The meeting organizers and an official from the DoD Office of Research and Advanced Technology worked out a compromise designed to salvage as many presentations as possible. After hectic review and revisions, 28 of the papers were presented in "closed" sessions, at which attendees were screened and required to sign the agreement used to control distribution of export-controlled DoD technical data.[15]

SPIE officials emphasize that the compromise was worked out in a friendly spirit and in good faith by both sides, but the society insists that the compromise was a "one-time necessity" and not a precedent. SPIE now dissociates itself from classified, controlled-access meetings or sessions that may be arranged by its members, but acknowledges that such meetings are held in parallel or immediately following societ y meetings and are regarded by many members as desirable and necessary.

Other professional societies admit uncomfortably to similar situations. They officially oppose and disclaim closed or limited access sessions that do not serve all members (especially when only non-U.S. citizens are excluded, since most identify themselves as international societies); yet recognize that such meetings are organized by members in parallel with society meetings—"a bit of a fiddle, one society official says. In 1984 the American Association for the Advancement of Science compiled a list of 12 events in which professional societies limited their traditional information dissemination function or activities to comply with security policies. For example, one session at a professional association meeting required participants to bring to the session proof of citizenship.[16] However, on September 17, 1985, a Joint Communication was sent to the Secretary of Defense from the elected presidents of 12 scientific and engineering societies, protesting DoD actions. It stressed the value to the Nation of open exchange of scientific information, pointing out that such exchange is necessary to validate findings, to cross-fertilize scientific knowledge and activity, and to avoid duplication of effort. The society president argued that secrecy hurts the national position in science, technology, and industrial competitiveness more than it strengthens national security. They notified the Secretary of Defense that they will not "be responsible for, nor will sponsor, closed or restricted-access sessions" in the future.[17]

DoD again, in April 1986, issued clarification of its procedures in screening papers on unclassified DoD-sponsored research for presentation at meetings. DoD says it will review papers under specific time frames (10 to 30 days) to help avoid last minute pressure for withdrawals. However, the statement also made clear that information deemed classified could be presented only on DoD premises, and unclassified information would still be subject to export control laws. Furthermore, the sponsors of scientific meetings are responsible for limiting access to authorized individuals (which societies say they cannot do).[18] Some DoD officials, and some "neutral observers," say that these actions have effectively alleviated professional concerns; a number of professional society officials consulted by OTA report that this issue remains one of active and strong concern to their societies and to most of their members. A nongovernmental science policy specialist asserts that DoD, in practice has been far less strict and less restrictive than their official policy guidelines and directives indicate they will be or should be. On the other hand, a scientist and society administrator argues forcefully that DoD policies have an "extraordinarily chilling effect" on scientific communication because scientists, fearful of prejudicing the essential source of funding for future research, lean over backwards and probably restrict themselves more than is absolutely required.

[15]This account was developed from discussions with both SPIE and DoD officials in May 1987 and differs in some details from accounts in the general and specialist media at the time (1985) and soon thereafter.

[16]Relyea, op. cit., 1986.

[17]American Association of Engineering Societies, *Policy* and *Engineering Priorities, 1986*, Washington, DC, 1986.

[18]Ibid.

The constitutional issue has not often been explicitly raised, possibly because Congress has appeared to add its authority to that of the executive agencies.

The export control statutes appear to provide a legal basis for restricting economic activities and scientific communication-formal and informal—within the United States as well as across its borders, since publication in U.S. journals is tantamount to worldwide publication. As already discussed, however, their constitutionality has not really been tested. The constitutional issue has not often been explicitly raised, possibly because Congress has appeared to add its authority to that of the executive agencies. Scientists instead have tended to try to minimize the opportunist y for government intervention through a strategy of "self -restraint."

SELF-RESTRAINT

The strategy of self-censorship could be a significant limitation on dissemination of scientific thought and on the exercise of constitutional freedoms.

The strategy of self-censorship poses an interesting ethical question. The objectives in self-censorship may be the exercise of reason, self-control, and patriotism, and the desire to avoid provoking authoritarian restrictions; but the end result could nevertheless be significant limitation on dissemination of scientific thought and on the exercise of constitutional freedoms.

In 1982, at the annual meeting of the American Association for the Advancement of Science (AAAS), CIA Deputy Director Admiral Bobby Inman said in a public address:

> A potential balance between national security and science may lie in an arrangement to include in the peer review process (prior to the start of research and prior to publication) the question of potential harm to the nation. 'g

Earlier, as Director of the National Security Agency (NSA), Inman had tried to take control over government-funded cryptography research from the National Science Foundation (NSF) .20 Having failed, he urged the American Council on Education to form a public cryptography study committee, which then recommended a voluntary system for prepublication review by NSA of manuscripts on cryptography. In 1981, NSF adopted a policy of requiring such prepublication review on "potentially classifiable results" coming from its research grants.

In his AAAS speech, Inman included not only cryptography but other areas in his argument for self-monitoring or self-censorship: computer hardware and software, electronic gear and techniques, lasers, crop projections, and manufacturing processes. He warned bluntly that if this was not done voluntarily, "public outrage' would produce laws further restricting publication of scientific work that government considered sensitive. Inman repeated this warning 3 months later at a congressional hearing held by two subcommittees of the House Science and Technology committee,[21] and said

[19]Relyea, op. cit., June 1986, p. 2.

[20]Competing scientific, industry, and national security interests in the development of encryption and related techniques and technologies for safeguarding data in computer and telecommunications systems has made this scientific technology particularly troubled by the tensions between national securit y restrictions and other societal priorities, as described in this chapter.

[21]U.S. Congress, House of Representatives, Committee on Science and Technology, Subcommittees on Science, Research, and Technology, and Investigation and Oversight, *Impact of National Security Considerations on Science and Technology Hearings*, 97th Cong., 2d sess., Mar. 29, 1982.

that unless Soviet access to American science, technology, and industrial information was voluntarily controlled, there would be a move by the government to further regulation.

Inman directly recognized that:

> . Science and national security have a symbiotic relationship. . . . In the long history of that relationship, the suggestion is hollow that science might (or should somehow) be kept apart from national security concerns, or that national security concerns should not have an impact on "scientific freedom."[22]

Protests were immediately raised about Admiral Inman's new call for self-restraint. The Executive Director of AAAS said:

> He has asked that research scientists submit voluntarily to open-ended censorship by the CIA or face the likelihood of being forced to do so by Congress. Even in wartime, such a demand would be an extreme one, and in the absence of national security emergency it is incongruous. It raises troubling questions involving both scientific freedom and the force of constitutional provisions against arbitrary government.[23]

[22] Inman, a statement in *Aviation Week & Space Technology*, "ClassifyingS cience: A Government Proposal. . . And a Scientist's Objection," Feb. 8, 1982, p. 10.

[23] Ibid., statement by William Carey, Executive Officer, AAAS.

NATIONAL SECURITY DIRECTIVES AND THE ROLE OF THE NATIONAL SECURITY AGENCY

National Security Directives

NSDD 84, in 1983 (discussed above), marked the first general public knowledge of National Security Decision Directives (NSDD) as a form of Presidential directive distinct from Executive Orders and Proclamations.[24] Executive Orders and Proclamations are always published. About 200 NSDDs have been issued by President Reagan since 1981, but only 5 have been publicly disclosed, the rest being classified. Between 1947 and 1981, other presidents had issued "National Security Action Memorandums" and "Presidential Directives" which like NSDDs were kept secret, from both the public and from Congress. They are all thought to be associated with the National Security Council, created within the Office of the President in 1947.

NSDD 189

In late 1982, after the recommendations of the Corson panel, President Reagan had ordered his Office of Science and Technology Policy (OSTP) to coordinate an interagency review

"It is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted."

of the issue of government secrecy (National Security Study Directive 14-82). The review was itself classified, so that there was no input from universities or other nongovernment sources. OSTP's report was due on March 1, 1983, but did not appear. There were rumors and stories in science policy newsletters that the Administration was about to announce new formal controls over "sensitive fundamental research," i.e., a fourth category of classification below that of "confidential." But such a strategy would involve both monetary and political costs. Classified information requires special procedures, controlled facilities, etc. Contractual agreements between researchers and funders are less expensive, legally defensible, and less likely to evoke protests.[25]

[24] Harold C. Relyea, Congressional Research Service specialist in American National Government, testifying before the House Committee on Government Operations on H.R. 145, Mar. 17, 1987. CRS press release.

[25] DoD was in fact considering a fourth security classification at this time, according to sources in the Pentagon, to protect "military operational data and high tech data—not fundamental research." (Communication to OTA May 1987.)

Instead of the long-delayed report from OSTP, in May 1984, DoD's Deputy Under Secretary for Research and Advanced Technology, Dr. Edith Martin, unexpectedly released a draft Decision Directive that was to become NSDD 189. Signed on September 21, 1985, NSDD 189 said:

> It is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted. ... Where the national security requires control, the mechanism for control of information generated from federally-funded fundamental research , . . at colleges, universities, and laboratories is classification. . . . No restrictions may be placed on conduct or reporting of [such] research that has not received national security classification, except as provided in applicable U.S. Statutes.

It was not clear what was encompassed in the term "fundamental research, " a term not until then in common use. Since the "applicable U.S. Statutes" include the Export Administration and Arms Export Control Acts, critics said that this directive did not materially change the existing situation, except that either more Federal agencies would have power to classify, or DoD's scope of authority would broaden. More scientists would become subject to NSDD 84 and be required to sign lifetime nondisclosure contracts. National security officials on the other hand deny this because "fundamental research" is excluded from export controls and there is no evidence that DoD is overusing classification procedures.

NSDD 189 was interpreted by some as an effort to "cool the campus secrecy issue" by dropping the idea of further controls in "gray areas' (between classified and unclassified research).[26] But in a memo accompanying NSDD, the White House stressed that it "preserves the ability of the agencies to control unclassified information using legislated authority provided expressly for that purpose in applicable U.S. statutes. "

A memorandum written by Under Secretary of Defense Richard DeLauer on October 1, 1984, to reassure the universities, again specified that no restriction would be put on publication of fundamental research sponsored by DoD. It defined fundamental research to include virtually all of that done on university campuses, with rare exceptions "where there is a likelihood of disclosing performance characteristics of military systems, or of manufacturing technologies unique and critical to defense." In these cases, restrictions must be put into the research contract.

The Role of the National Security Agency

The Brooks Act of 1965 gave the National Bureau of Standards authority for developing technical standards for computer systems. Private firms were developing an interest in this market, and commercial security devices meeting NBS standards were developed for computers. During the mid-1970s, a government-certified cryptographic algorithm and a' 'public-key" algorithm were announced (in the open literature), and inexpensive security devices were developed commercially.

Presidential Directive/National Security Council 24 (PD/NSC-24), issued by President Carter in 1977, said that nongovernmental telecommunications information "that would be useful to an adversary" would be identified, and the private sector informed of the problem and encouraged to take appropriate actions.[27] This was a clear sign that the Federal Government, DoD in particular, would take a stronger hand in telecommunications security.

The Secretary of Defense was to be responsible for protecting government communications, both classified and now "unclassified but sensitive" communications. The Secretary of Commerce would be responsible (through NTIA) for government-derived unclassified data not related to national security, and would

---

"*Science and Government Report, "White* House Decides To Cool Campus Secrecy Issue," vol. XIV, No. 11, June 15, 1984; Colin Norman, "Universities Prevail on Secrecy, " *Science,* vol. 226, No. 26, October, 1984, p. 418.

"National Telecommunications Protection Policy (unclassified), Feb. 9, 1979, unclassified excerpts from Presidential Directive/NSC-24, Nov. 16, 1977, classified.

NSDD 145 worried civil libertarians because of the broad scope of nonclassified information to be protected and because of the central role given to NSA, an agency outside of the usual modes of accountability.

deal with the private sector to "enhance their communications protection and privacy. " The Defense and Commerce Departments attempted to develop a joint proposal for a national policy on cryptography but were unable to reach agreement, They submitted separate proposals which, however, were never acted on by the President's Science Advisor.[28]

NSDD 145 and HR 145

National Security Decision Directive 145 (NSDD 145), September 17, 1984, superseded PD/NSC-24, and made NSA the central agency ("Executive Agent") for development and choice of cryptography-based technology for the security of unclassified, but sensitive information in telecommunications and computer systems of all government agencies.* This seems to apply whether the information concerns national security or not, and regardless of whether the technology is to be used for security or for authenticating transactions.

In short, NSDD 145:

- broadened NSA protection to encompass unclassified information in telecommunications and automated information systems;
- assigned to NSA the full responsibility for developing and advising of safeguard technology and for making decisions about technical standards, ignoring the role of NBS under the Brooks Act; and
- established an interagency group to implement and enforce NSDD 145 policy.

This announcement worried civil libertarians because of the broad scope of nonclassified information to be protected and because of the central role given to NSA, an agency outside of the usual modes of accountability. From the time it was issued, there have been conflicting interpretations and official pronouncements about the details of what it means. At first, "sensitive information" was defined as "unclassified but sensitive national-security-related information. " In June 1985, Donald Latham, Assistant Secretary of Defense and Chairman of the National Telecommunications and Information Systems Security Committee (NTISSC) established under NSDD 145, said that "sensitive" information might include anything from crop forecasts to personnel records.[29] Three months later, in testifying before the Committee on Government Operations, September 18, 1985, Mr. Latham said specifically that "non-national-security-related information was not included in the purview of NTISSC. But in October 1986, an NSA memorandum, NTISSP No. 2,[30] extended this purview to:

> Other government interests . . . related but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. government by its citizens (Section II, Definitions).

The NSA policy announcement also said:

> The NSDD-145 Systems Security Steering Group has established that sensitive, but un-

[28] For a more detailed treatment of the Government's role in computer and communications security, see U.S. Congress, Office of Technology Assessment, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information,* OTA-CIT-31O (Washington, DC: U.S. Government Printing Office, October 1987).

*The National Security Agency was established by Executive Order in 1952, during the "Cold War, " to carry out "signals intelligence' against hostile countries (i.e., to intercept and decode information they were sending through electronic communications) and to safeguard U.S. classified information against similar actions by those countries.

[29] U. S. House of Representatives, Committee on Science and Technology, Subcommittee on Transportation, Aviation, and Materials, *Hearings on Computer Security Policies,* June 27, 1985, statement of Donald Latham.

[30] National Policy on Protection of Sensitive but Unclassified Information in Federal Government Telecommunications and Automated Information Systems, NTISSP No. 2, Oct. 29, 1986,

> classified information that could adversely affect national security or other Federal Government interests shall have system protection and safeguards; however the determination of what is sensitive but unclassified information is a responsibility of Agency heads.

It now appears that the definition of "sensitive" could be applied to almost any information, or at least a very broad range of information, even if it is already published or available. NSDD 145 applies not only to Federal agencies but also to their contractors who electronically transfer, store, process, or communicate sensitive but unclassified information. It gives NSA the dominant role in developing the technology to be used, or deciding which technology will be used, by private sector organizations affected by the directives. NSA and DoD, however, emphasize that "protection' in this context literally means guarding against unauthorized access and malicious misuse by 'hackers. "

This new role for NSA would have gone beyond *development of technology* to involvement in decisions about the *content* of information, in order to prescribe what kind of security is appropriate. In late 1985 there had been signs of renewed government concern about the "leakage' of information from campuses and through commercial databases. The Pentagon released a CIA report, *Soviet Acquisition of Militarily Significant Western Technology: An Update,* based on Soviet documents. It listed 62 American universities "targeted for scientific and technical espionage" aimed at information about applied technology and engineering but also including "fundamental research for both Soviet military- and civilian-related science developments. " This scientific and technological data is often in commercial electronic databases providing services to business and the public:

> The individual abstracts or references in government and commercial data bases are unclassified, but some of the information, taken in the aggregate, may reveal sensitive information concerning U.S. strategic capabilities and vulnerabilities. . . .[31]

[31] *Science and Government Report,* Oct. 1, 1985. The report released by Secretary of Defense Weinberger was an "update" of a declassified Central Intelligence Committee report originally released in 1982 by the Senate permanent subcommittee on Investigations. Dan Morgan, "Stolen U.S. Technology Boosts Soviet Strength, Report Says, " *Washington Post, Nov. 15, 1982.*

There is a strong concern that DoD may require private sector database operators, at a minimum, to provide the government with lists of their subscribers, to place limits on foreign subscribers, and to increase the use of password protection and encryption.

The report went onto say that "One solution appears to be to thoroughly screen all candidate database entries and keep sensitive government information out of the public databases . . ." but added, "Unfortunately, this may also inhibit the United States' own national research effort by resisting the ready availability of such information. "

It was clear that NSDD 145 had already given NSA the decisive role in prescribing security measures for government's automated databases, as well as telecommunication systems, but its authority over commercial databases is still in dispute. Diane Fontaine, director of information systems in the office of the Assistant Secretary of Defense, reportedly said at a meeting of the Information Industry Association, November 11, 1986: "The question is not should there be limits [on information in commercial databases] but instead what those limits should be."[32] Ms. Fontaine has since stated that she was misquoted and was referring only to government databases, but many auditors understood the reference as being to commercial databases. There is a strong concern that DoD may require private sector database operators, at a minimum, to provide the government with lists of their subscribers, to place limits on foreign subscribers, and to in-

[32] Quoted by Johanna Ambrosio, "Attempts To Restrict Private Data Bases Vex Industry, *Government Computer News,* Dec. 15, 1986. Another reporter's version was "The question is not whether we are going to protect information; the question is where the controls will be applied. " Irwin Goodwin, "Making Waves: Poindexter Sails Into Scientific Data Bases, *Physics Today,* January 1987, p. 52.

crease the use of password protection and encryption.

In 1986 there were 3,200 electronic databases available worldwide through 486 online information services; 70 percent of these databases are produced in the United States, and all but two of the 20 largest database companies are American corporations.[33] Throughout much of 1986, a U.S. Air Force team visited commercial database owners to inquire about the extent of foreign access to these databases.[34]

Nonclassified government databases, even those specifically set up to provide better public access to information that is in the public domain, are in some cases already restricting access. An internal NASA memo of September 29, 1986, labeled "The So-called 'No-No' list,"[35] provides names of 33 organizations or individuals who are not to be "provided with subscriptions to NASA Tech Briefs, technical support packages, or other Technology Utilization documentation. " The memo adds that "all embassies and consulates in the U.S. and representatives of foreign companies or organizations are to be included in this list. " NASA Technology Utilization is a service to disseminate technical information to the public. Its information is not classified.

As major opposition to the thrust of NSDD 145 developed within Congress, a new National Security Advisor, Frank Carlucci, who had succeeded Mr. Poindexter, decided to review NSDD 145. His "key objective [was] finding a mechanism to eliminate any possible ambiguity regarding the role of the National Security Advisor in connection with the System Security Steering Group, " and Carlucci instructed his staff "to initiate the procedure and prepare the papers necessary to rescind NTISSP 2.[36]

H.R. 145

NSA had expanded its role into areas legislatively assigned to the National Bureau o Standards (NBS). H.R. 145, the Computer Security Act of 1987, was accordingly introduced It would assign to NBS the responsibility for developing and promulgating standards and guidelines for safeguarding unclassified sensitive information in Federal systems, and for helping both civilian agencies and the private sector in using computer security safeguards.[37] This bill was passed by the House in July 1987 but had not been taken up by the Senate a of early January 1988.

---

[33]Information supplied by Information Industry Association, See *Potential Government Restrictions on United States Unclassified Commercial* Databases, Mar. 9, 1987, available from the association.

[34]Ibid., see also: Michael Schrage, "U.S. Seeking To Limit Access of Soviets to Computer Data, " *Washington Post,* May 27, 1986; and "Are Data Bases a Threat to National Security, " *Business Week,* Dec. 1, 1986, p. 39. But DoD officials describe this as "data gathering with no purpose related to immediate actions. " (In communications to OTA, May 1987.)

[35]Signed by Walter M. Heiland, Manager, Technology Utilization Office, and addressed to "All TU Officers, IAC Directors and Other Members of the TU Family, " and reprinted by *Translational Data and Communications Report,* February 1987, p. 21.

Wetter from Frank C. Carlucci, National Security Advisor The White House, to the Hon. Jack Brooks, Chairman, Committee on Government Operations, U.S. House of Representatives, Mar. 12, 1987.

[37]Hearings on HR 145 were held on Feb. 26 by the Subcommittee on Legislation and National Security, Committee on Government Operations, U.S. House of Representatives. The White House accepted this measure and the bill was passed by the House in July 1987, and is still waiting to be introduced in the Senate as of early January 1988.