Michigan Journal of International Law

Volume 16 | Issue 2

1995

U.S. Government Control Over the Export of Scientific Research and Other Technical Data: Holes in the Sieve

Robert Greenspoon
University of Michigan Law School

U.S. GOVERNMENT CONTROL OVER THE EXPORT OF SCIENTIFIC RESEARCH AND OTHER TECHNICAL DATA: HOLES IN THE SIEVE

*Robert Greenspoon**

INTRODUCTION

The main theme of U.S. export restrictions is the non-proliferation of sophisticated weapons systems to inimical countries.[1] The web of export regulations which governs these restrictions is intended to promote national and international security. Because weapons development feeds upon scientific advance, the control of weapons technology necessarily brings with it the control of science itself. Resistance to such control comes from two sources: academia, because of its norms in favor of intellectual freedom, and industry, because of its norms in favor of the freedom of markets. This Note addresses the question of whether export restrictions on scientific data are appropriate and tenable.

In Part I, I establish the backdrop for answering the question by describing the kinds of scientific data that might be subject to security classification and export licensing. In Part II, I outline briefly who chooses what should be restricted and who enforces these restrictions. In Part III, I describe several situations in which the federal government has vigorously enforced controls over the dissemination of scientific information. I also analyze two recent cases involving computer software that I believe analogize directly to the scientific endeavor. Finally, in Part IV, I explain why First Amendment barriers, the growth of the Internet global computer network, and cultural values peculiar to the scientific community should assuage most concern about categorizing scientific research data for national security purposes.

---

* J.D., University of Michigan (1995); A.B., University of Chicago (1992). The author would like to thank Professor Rebecca S. Eisenberg, for whose seminar this note was originally prepared. The author also thanks Gavin Domm, Michael Edmunds, John Felitti, Beth Fulkerson, Daniel Ginsberg, and Paul Tauber for their helpful suggestions. Finally, the author thanks John J. Molenda for his friendship and support during the entire project.

1. *See, e.g.*, Export Administration Regulations, 15 C.F.R. § 778.1(a) (1994) (defining "the types of transactions that are governed by the U.S. policy concerning the non-proliferation of chemical and biological weapons, nuclear weapons or explosive devices, missiles systems and the U.S. maritime nuclear propulsion policy."). The export regulations described in this note derive from the power of the President to make foreign policy. *See* U.S. CONST. art. II, § 2.

I. SCIENCE SUBJECT TO EXPORT CONTROL

A. *Control by Security Classification*

As a general matter, the federal government has two routes by which it can prevent the export of scientific data — through security classification or through export licensing. In 1985, to quell concern that fundamental research might be chilled by export or publication restrictions, President Reagan issued a directive on scientific data setting forth the Executive's presumptive hands-off approach. This directive states that "to the maximum extent possible, the products of fundamental research [should] remain unrestricted. . . . [T]he [preferred] mechanism for control of information generated during federally funded fundamental research in science, technology, and engineering at colleges, universities and laboratories is classification."[2] The directive goes on to state that no restrictions on the conduct or reporting of unclassified research may be imposed, "except as provided in applicable U.S. statutes."[3] In effect, this directive provides that any U.S. government agency which supports scientific research by funding or by contract must classify the research results if national security might be threatened by publication.[4]

In addition to formal classification by the designations "confidential," "secret," or "top secret," certain data may be declared "sensitive." Sensitive but unclassified information is defined as "information the disclosure, loss, misuse, alteration, or destruction of which could adversely affect national security or other Federal Government interests."[5] As a practical matter, data declared as sensitive (i.e., nominally without particular restrictions on export) will more readily become classified than non-sensitive data during the regular agency reviewing process. Because the definition is broad, and because agency discretion may go

---

2. Sensitive Technologies from Federally Funded Research, Statement by the Principal Deputy Press Secretary to the President, 21 WEEKLY COMP. PRES. DOC. 1147 (Sept. 27, 1985).

3. *Id.* at 1148. This caveat allows export control statutes to apply to federally funded research that goes unclassified.

4. It is difficult to find an explicit definition of "national security." When speaking about export restrictions, one must be satisfied accepting an operational definition such as, "that which individuals in government assert is national security." Such decisions are apparently made on an agency by agency basis. *See* Note, *The National Security Agency and Its Interference With Private Sector Computer Security*, 72 IOWA L. REV. 1015, 1034–36 (1987) [hereinafter *NSA Interference*].

5. NATIONAL POLICY ON PROTECTION OF SENSITIVE, BUT UNCLASSIFIED INFORMATION IN FEDERAL GOVERNMENT TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS, NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY POLICY NO. 2, § II (Oct. 29, 1986) (quoted in *NSA Interference*, *supra* note 4, at 1035).

unreviewed in the classification reviewing process,[6] ultimately the amount and scope of information that becomes classified increases as more information is declared to be sensitive.[7]

B. *Control by Export Licensing*

In addition to security classification, export licensing is the other route to U.S. governmental control over scientific and technical information. Unlike most restrictions arising from classification, licensing restrictions may be imposed upon information which is generated by private industry or by non-government funded academic research. Several statutes operate to restrict the export of scientific information notwithstanding the availability of licensing rights. For example, under the Invention Secrecy Act,[8] a government agency may classify a patent application and delay the issuance of a patent if the invention's dissemination threatens national security. Under the Atomic Energy Act,[9] information about atomic energy is probably considered "born classified," no matter what its source.[10] The act with the broadest application to scientific research is the Export Administration Act[11] (hereinafter EAA). Under the EAA, the Department of Commerce issues export licenses on all exports so that the federal government may maintain control over national security, foreign policy, and short supply situations.[12]

A short exposition of definitions and of types of export licenses will illustrate that scientific research results are subject to varying degrees of treatment under the EAA, depending on how proximately aligned the information is with weapons technology. "Export" of information can be a shipment of data to another country, a "release" of data with knowledge or intent that it arrive in a foreign country, or a "release" in a foreign country.[13] A "release" is a (i) visual inspection by foreign nationals of U.S.-origin equipment and facilities; (ii) oral exchanges of information in the United States or abroad; or (iii) the application to

---

6. *See NSA Interference, supra* note 4, at 1036.

7. *Id.*

8. 35 U.S.C. §§ 181–88 (1988).

9. 42 U.S.C. §§ 2011–2296 (1988).

10. *See* Peter Swan, *A Road Map to Understanding Export Controls: National Security in a Changing Global Environment*, 30 AM. BUS. L.J. 607, 613 (1993), (citing *The Government's Classification of Private Ideas: Hearings Before a Subcommittee of the House Committee on Government Operations,* 96th Cong., 2d Sess. 144 (1981)).

11. 50 U.S.C. app. §§ 2401–2420 (1988, Supp. I 1989, & Supp. II 1990).

12. *See* Swan, *supra* note 10, at 617–26. Only national security and foreign policy appear germane here, as "short supply" of knowledge is an incoherent idea.

13. *See* 15 C.F.R. §§ 779.1(b)(1).

situations abroad of personal knowledge or technical experience acquired in the United States.[14] Technical data includes "[s]pecific information necessary for the 'development,' 'production,' or 'use' of *a product.*"[15]

Under the foregoing definition of technical data, all scientific research results, except those which have no application to the fashioning of "a product," are subject to Department of Commerce licensing for export. The technique used in the regulations is to create a blanket prohibition against the export of all technical data and then to delineate the categories of technical data which may overcome this prohibition via various types of licenses.[16] Technical data can only be exported under a validated license unless the regulations otherwise provide.[17] A validated license, as might be expected, is one requiring submission to the Office of Export Licensing of a formal application containing detailed information about the recipients of the data and the uses to which the data will be put.

1. Exceptions to the Filing Requirement for an Export License: GTDR, GTDU, and GTDA

Within the regulations, specific and general exceptions have been carved out of the blanket requirement of filing for a validated license for technical data, and hence scientific research, export. These exceptions from the filing requirement are embodied in the "general technical data" licenses: GTDR, GTDU, and GTDA. Export under these exceptions still carries all of the legal consequences of exporting under a validated license (including the possibility of revocation), even though an application need not be filed.

GTDR and GTDU licenses apply to technical data of specific types named as eligible on the Department of Commerce's Commodities Control List (CCL),[18] and are available for export of data only to "good" countries, as described below. GTDR licenses require the exporter to obtain specific written assurances from the foreign importer that the data will not be released to "bad" countries. GTDU licenses usually involve

---

14. *Id.* § 779.1(b)(2).

15. *Id.* § 779.1(a) (emphasis added) (incorporating within "technical data" the definition of "technology" found in 15 C.F.R. § 799.1, Supp. 3). The 1994 Export Administration Regulations hint that the definition of "technical data" will undergo revision in the near future. *Id.* § 779.1(a). As of March 29, 1995, this revision has not yet been released.

16. *Id.* § 770.3(a).

17. *Id.* § 779.5(a).

18. *Id.* § 799.1, Supp. 1.

de minimis transfers to foreigners of information, such as information contained in operation technical data, sales technical data, or software updates.[19] Because these transfers are trivial, and collecting foreign assurances would be burdensome, GTDU licenses require no written assurances that bad countries will not receive the data, although penalties still can be imposed for knowing release of the data to unauthorized parties.

GTDA licenses, when applicable, may be considered general, in contrast to specific, exceptions to the requirement for a validated export license. Data falling within the ambit of a GTDA license may be exported anywhere, and the exporter need neither file an application in the Department of Commerce nor acquire non-transfer assurances from foreign importers. The licensing regulations enable most scientific research to be released under the nonrestrictive GTDA scheme. Four kinds of technical information may be exported under a GTDA license: information resulting from fundamental research, information that is already or will be made publicly available, educational information, and information in connection with certain patent applications.[20]

Scientific research primarily falls within the first two classes of technical information. For example, foreign publication of research results should usually be unproblematic: notwithstanding other restrictions, such as classification, submission of scientific research results to a foreign journal for the purposes of publication will usually fall under one or more GTDA licensing classifications. If the research is nonproprietary, then it is exported under a GTDA license because it is considered fundamental research.[21] Even if the research is proprietary, such as research carried out for the purposes of fashioning a commercial product, it will fall under the GTDA license if sent to a foreign journal because then it becomes information that will be made publicly available.[22]

The same logic applies to open scientific conferences, no matter where they are held. So long as a conference is open, then proprietary or fundamental research can be presented under a GTDA license. Unless exported information qualifies under one of the four kinds of technical data outlined above which comprise the general exception GTDA category, either the validated license or the more restrictive GTDR or GTDU license is required for its export.[23]

---

19. *Id.* § 779.4.

20. *Id.* § 779.3(a).

21. *See id.* § 779.3(c). This provision also addresses how to treat joint industry-academia research ventures regarding GTDA eligibility. *Id.*

22. *See id.* § 779.3(b).

23. *Id.* §§ 779.3(b), 779.3(c). *See also id.* § 779.3(f)(2). If government contract re-

2. Country Categories Determining which License Applies to Particular Technical Data

The U.S. categorizes "bad" countries within a handful of lettered categories which reflect generally the nature and extent of export restrictions.[24] The countries seemingly most inimical to U.S. interests are listed in categories S and Z: Cuba, Libya, and North Korea. Thus if particular technical information is denominated SZ-restricted only, then under a GTDR license, it can usually be sent to any country except Cuba, Libya, and North Korea; an application for a validated license would have to be filed to export it to the SZ group members. Such information is not very restricted. If particular technical data is listed as QSTVWYZ-restricted, then under a GTDR license, it can usually be sent to any country not named in the regulations within the lettered groups. Otherwise, a validated license application would have to be filed. Such information is very restricted.

A casual perusal of the specific controls imposed upon the numerous commodities listed in the regulations suggests that the scope of restriction corresponds generally to the ease of military application and the danger of misuse of the technical information involved.[25] Even if the technical data will never leave the country, licensing regulations may be a consideration whenever foreign nationals are allowed to work on a project which would require a GTDR, GTDU, or validated license if results were exported.[26] Both validated and general licenses are subject to revocation at any time without notice.[27] The revocation provision does not address the standard by which a license may be revoked.[28] A different section of the regulations establishes the vague standard that ship-

---

strictions on publication or export apply to otherwise GTDA-eligible scientific research results, then "[s]pecific national security controls" must be agreed upon in the government research contract. "A general reference to one or more export control laws or regulations or a general reminder that the Government retains the right to classify is not a 'specific national security control.'" *Id.*

24. *See id.* pt. 770, Supp. 1; 59 Fed. Reg. 6,524 (1994) (to be codified at *id.*) (removing Vietnam from country group Z to country group Y).

25. *See, e.g., id.* § 799.1, Supp. 1.

26. *See id.* pt. 779, Supp. 5 (answering common questions regarding licensing, including many questions concerning the conditions under which the involvement of foreign nationals necessitates a validated license). In such a case, the nationality of the foreigner may be key. *Id.*

27. *Id.* § 770.3(b). I can imagine a casual and unsophisticated exporter being taken by surprise when a GTDA license not even applied for is revoked without notice. Such a surprised response would probably be similar to that observed of the optical engineers when the Department of Defense cracked down on the presentation of scientific papers at an open conference in 1982, as described *infra* part III.

28. *See* 15 C.F.R. § 770.3(b).

ments may be prohibited "whenever there is reason to believe that the export regulations have been, or will be violated."[29]

II. Creation and Enforcement of Restrictions

Jurisdiction over export restrictions is shared by the Departments of Commerce, State, and Defense.[30] Additionally, the United States is a member country of the Coordinating Committee of the Consultative Group (COCOM), which is a multilateral organization that monitors and restricts the distribution of military technology to countries outside the group.[31] Although restrictions may be placed on individual exports on a case-by-case basis under the EAA, either by the Secretary of Commerce or by the President on the recommendation of the Secretary of Defense,[32] the "heart of the control scheme is the Commodity Control List (CCL)."[33] This list is updated at least every three years for items that are subject to multilateral control, and annually regarding items that are subject to domestically fashioned restrictions.[34] The authority to do so is vested in Technical Task Groups (TTG's) which are "composed of technical representatives of various government agencies."[35] In updating the CCL, the TTG's consider several factors in reviewing items, including civilian uses, military uses, technological state of development, and availability abroad.[36]

A person found in knowing violation of the EAA (e.g., exporting technical data under a GTDR license with knowledge that it will be reexported to a forbidden recipient in violation of the regulations) may be fined five times the value of the exports or $50,000, whichever is

---

29. *See, e.g., id.* § 771.2(c)(1).

30. The Department of Commerce administers the EAA, *supra* note 11; the Department of State administers the Arms Export Control Act, 22 U.S.C. §§ 2777-79 (1988, Supp. I 1989, & Supp. II 1990), which authorizes the creation of the Munitions Control List; and the Department of Defense, among others powers, has the authority to "review any proposed export of any goods or technology to any country to which exports are controlled for national security purposes . . . to recommend to the President that such export be disapproved." EAA, 50 U.S.C. app. § 2409(g).

31. *See* Swan, *supra* note 10, at 619-21. The group is currently composed of Australia, Belgium, Canada, Denmark, France, Germany, Greece, Italy, Japan, Luxembourg, the Netherlands, Norway, Portugal, Turkey, the United Kingdom, and the United States. *Id.* at 619. The last meeting of COCOM adjourned on March 31, 1994. *See* 59 Fed. Reg. 25,303 (1994).

32. *See* 50 U.S.C. app. § 2403-1(c).

33. Swan, *supra* note 10, at 625.

34. 15 C.F.R. § 770.1(b)(1).

35. *Id.* § 770.1(b)(2).

36. *Id.* § 770.2(b)(3).

greater.[37] An individual found in willful violation of the EAA may be fined up to $250,000 or imprisoned 10 years or both. Other persons may be fined five times the value of the exports or $1,000,000, whichever is greater.[38] Administrative sanctions for violators may also come into play, such as debarment of an exporter from licensing eligibility.[39] Persons who disclose information relating to the national defense (i.e., classified information) to unauthorized parties are subject to a fine, imprisonment for up to 10 years, or both.[40]

III. Examples of Controlled Scientific Information

Examination of specific instances of U.S. government classification and export regulation of scientific and technical data give a clearer picture about whether such controls are appropriate and tenable, given the clash of scientific and market values against the national security mandates. These examples include the federal government's successful attempt to have withdrawn over 150 papers from an open conference on advanced optics, its unsuccessful attempt to induce U.S. research universities to monitor the activities of foreign national scientists, and the indeterminate outcome of the case of *United States v. Progressive, Inc.*[41] Some more recent examples involving computer software illustrate potential government threats to the right to communicate scientific and technical data, and evidence reasons to believe that export controls will not chill academic or market freedoms. These latter examples include the GURPS Cyberpunk raid on Steve Jackson Games, Inc., and the ongoing criminal investigation involving the dissemination of the encryption scheme, "P.G.P." Part IV, *infra*, will address the significance of these examples of government enforcement of controls over technical information.

A. *Society of Photo-Optical Instrumentation Engineers*[42]

In 1982, the Society of Photo-Optical Instrumentation Engineers (SPIE) held an open conference in San Diego at which about 700 unclassified papers were to be presented to scientists from 25 countries,

37. 50 U.S.C. app. § 2410(a).

38. *Id.* § 2410(b).

39. *Id.* § 2410(c).

40. 18 U.S.C. § 793 (1994).

41. 467 F. Supp. 990 (W.D. Wis. 1979).

42. This account is from M. Christina Ramirez, *The Balance of Interests Between National Security Controls and First Amendment Interests in Academic Freedom*, 13 J.C. & U.L. 179, 189–91 (1986).

including communist bloc countries. About one week before the conference began, the Department of Defense (DOD) contacted the organizers to request a room in which they could interview DOD-funded scientists to determine whether they had followed appropriate classification procedures according to their funding contract. Panic ensued. The clear message received by the scientists was that if they did not follow appropriate classification procedures, then the reading of research results that should have been classified would result in criminal sanctions.[43] This caused over 150 papers to be "voluntarily" withdrawn by scientists uncertain about whether they had followed proper procedure and who were unwilling to risk criminal sanctions had they not. Ironically, a DOD official intimated that if all of those scientists had followed the right procedures, the DOD would not have been able to handle the workload. In all likelihood, some of the withdrawn papers did contain classifiable information under the terms of the funding grants and should not have been presented. However, the scientists' inexperience with information control and unwillingness to go to prison for possible violations of national security probably caused a large number of unclassifiable papers to be withdrawn.

B. *University Recalcitrance about Enforcing Visa Restrictions*[44]

The federal government has been less successful in another attempt to tighten national security controls on scientific information. The State Department's authority to impose restrictions on the activities of foreign nationals admitted to study in U.S. universities has been used as an *ex ante* means of curtailing the release (and thus the export) of classified or restrictable information. Complete enforcement of these restrictions is a practical impossibility, which is why the State Department has attempted to enlist the aid of the universities themselves. In response to a 1981 request that the University of Minnesota enforce security restrictions on a visiting Chinese scientist, the president of that university wrote that the mission of the university is to teach and that university employees were not hired to enforce government-imposed restrictions on visiting scholars. The president of Stanford University noted that the State Department's similar requests to him were "outlandish," especially a mandate to keep a visiting expert in robotics from speaking with anyone

---

43. Because this was an open conference, any research results could be read with impunity under the GTDA licensing regime so long as whatever security provisions that existed in the government funding contracts were followed. *See* 15 C.F.R. § 779.3; *supra* notes 20–23 and accompanying text.

44. *See generally* Ramirez, supra note 42, at 202–04.

working in Silicon Valley. In still another example, a Massachusetts Institute of Technology professor received a set of questions from the State Department regarding the activities of a visiting scholar from Beijing. The professor did not answer the questions and had no further contact with the State Department regarding that scholar. These examples illustrate anecdotally the unwillingness of universities and individual professors to police government security regulations covering the activities of foreign nationals who might gain technical data that would constitute an unauthorized export.

C. *The* Progressive *Case*[45]

While government attempts to exert control over scientific information were successful in the case of the SPIE, and apparently unsuccessful in the case of enlisting universities to police the activities of foreign nationals, it is unclear in the case of *United States v. Progressive, Inc.*[46] whether the government has acquired any leverage for such control from the courts. The Progressive magazine assigned a journalist to write an article designed to illustrate to readers the extent of the government's authority and willingness to censor the press in the name of "national security." The article was to be entitled, "The H-Bomb Secret: How We Got It, Why We're Telling It." The journalist, using solely unclassified and public record materials, such as physics textbooks and encyclopedias, wrote a compilation on how to build a hydrogen bomb. The United States sued in district court to enjoin the publication of that article on the grounds that the information contained within it was classified. On a preliminary injunction, the district court agreed with the United States, holding that the government would probably succeed on the merits in its contention that it is possible for a collection of unclassified information to become classified if those pieces taken as a whole are already classified. The case never went to trial because the issue was mooted when in the course of reporting on the case, other periodicals not subject to injunction reported essentially the contents of the Progressive's article. It is unclear whether this holding, if made permanent on a full review, would be a prior restraint in violation of the First Amendment protection of free speech. If not a violation, it would be another means by which a private cataloguing of technical information could be curtailed by national security restrictions.

---

45. *See generally id.* at 222–24.

46. 467 F. Supp. 990 (W.D. Wis. 1979).

D. *Recent Enforcements: GURPS Cyberpunk and P.G.P.*

Whereas the examples above took place while the cold war was the major motivation for U.S. foreign policy,[47] two recent criminal investigations involving computer software evidence how the public and the targeted parties react when academic and market freedoms are threatened by federal government controls. Even though both investigations involve private commercial matters, the reactions of the targeted parties analogize well to the hypothetical response of scientists under similar pressures who hold similar attitudes and values.

1. GURPS Cyberpunk[48]

A small company in Austin, Texas, named Steve Jackson Games, Inc. (SJG), publishes a role playing game system entitled, "General Universal Role Playing System" (GURPS). In 1990, they were about to publish and market the "Cyberpunk" version, so called after the genre of science fiction, popularized by author William Gibson,[49] in which computer hackers and corporate megaliths ally themselves to share control of the levers of power over society. Players of this game assume the roles of corporate executives, computer hackers, or other ne'er-do-wells of this society, and pretend to interact in a fictional neo-apocalyptic future where high technology used for low purposes sets the tone of human relationships. On March 1, 1990, the United States Secret Service raided the SJG offices and seized computer equipment and company documents. The company was forced to suspend operations for a month, postpone release of the new GURPS, and lay off half its employees while the Secret Service inspected the impounded documents. No charges were ever filed, although it is conceivable that the Secret Service was investigating for violations of the EAA or for releasing U.S. government classified information. After drawing the computer culture's attention to the power of the government to restrict content in commercial "speech" during the progress of a criminal investigation, SJG suc-

---

47. *See generally* Swan, *supra* note 10, at 607–26.

48. *See generally* Gregory E. Perry and Cherie Ballard, *A Chip by Any Other Name Would Still be a Potato: The Failure of Law and Its Definitions to Keep Pace with Computer Technology*, 24 TEX. TECH L. REV. 797, 804–06 (1993).

49. *See* WILLIAM GIBSON, THE NEUROMANCER (1984). The cyberpunk culture itself is undergoing a personality evolution, as more people connect on-line onto the Internet global computer network and begin to enter a world of seemingly unlimited access to information and seemingly unlimited audiences for self-expression. This is known as cyberspace. *See* Philip Elmer-Dewitt, *Cyberpunk!*, TIME, Feb. 8, 1993, at 58.

cessfully sued the U.S. government for damages incurred during the impoundment of its property.[50]

Although the search warrant was issued under seal and has not been unsealed, the raid apparently occurred because an employee of SJG ran a public bulletin board system (BBS) onto which a real-life computer hacker had transmitted a stolen computer file. This computer file was stolen from the Bellsouth Regional Bell Operating Company's computers in Atlanta and contained proprietary information regarding the operation of the 911 emergency system. The Secret Service (which is the federal agency charged with investigating most computer crimes) traced the file to the SJG employee's BBS and subsequently began investigating his employer as well.

SJG also ran a public BBS, and the Secret Service must have logged onto it in the course of investigating the SJG employee. What they thought they encountered was a computer BBS with a great deal of technical information on computer security, how to break into computer networks, and about "cyberpunk" computer hacker culture itself. What they actually encountered was an on-line version of the new GURPS publication that SJG always made available prior to releasing the book form of the new version. This public pre-publication on-line version was intended to invite consumer response to new products. Instead it invited a search by Secret Service agents, who may have thought they had hit the nerve center of computer crime in the United States.

2. P.G.P.

The National Security Agency (NSA) is the intelligence arm of the federal government entrusted with eavesdropping on the world's electronic communications.[51] It is responsible both for ensuring the impregnability of U.S. secret communications and for cracking the codes protecting those of other countries.[52] Computer data transmissions also fall under this NSA mandate.

Currently the highest level of computer data encryption is an algorithm called DES. It is commonly believed that the NSA is capable of easily breaking this code, thereby enabling it to intercept any data

---

50. Steve Jackson Games, Inc. v. U.S. Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993), *aff'd* 36 F.3d 457 (5th Cir. 1994).

51. *See* John P. Barlow, *Decrypting the Puzzle Palace*, COMMUNICATIONS OF THE ACM, July 1992, at 25. The NSA intercepts every electronic message that goes out of the United States and, although prohibited by law from doing so, some that are entirely domestic, using its 12 underground acres of super computers to sort through them. *Id.*

52. *See NSA Interference, supra* note 4, at 1020–24. *See also* John Carey, *Spy Vs. Computer Nerd: The Fight Over Data Security*, BUS. WK., Oct. 4, 1993, at 43.

protected by DES.[53] It is illegal to export DES in any computer-related product or by itself without special permission from the State Department because encryption algorithms are on the Munitions Control List and therefore not subject to export at all.[54] In general, it is illegal to export any data encryption scheme. United States software and telecommunications companies have chafed under this restriction and claim that because they must make exportable versions of their products with extremely weak security encryption, they are losing huge revenues to European companies who are not under such restrictions in their worldwide sales.[55] Consumers abroad want their communications protected, and U.S. companies are not allowed to provide it.

Several years ago, Philip Zimmerman, an independent U.S. programmer, created an encryption algorithm called P.G.P. (standing for "Pretty Good Privacy"). It can easily be incorporated into computer software and is apparently at least as secure as DES. This program has been freely distributed around the world and is used on thousands of personal computers to protect against eavesdropping. On September 9, 1993, two companies which plan to license the program for use in software, Viacrypt of Phoenix, Arizona, and Austin Code Works of Austin, Texas, were issued subpoenas by a federal grand jury. This criminal investigation is intended to determine whether these two companies are in violation of U.S. export restrictions by licensing the use of P.G.P. in products which they know will be exported.[56]

IV. HOLES IN THE SIEVE

The examples above, while anecdotal, illustrate situations in which government control has clashed with academic and market freedoms. They do not, however, reflect any clampdown by the federal government that would greatly influence U.S. science or U.S. industry. First Amendment protections, the easy worldwide dissemination of data over the Internet, and cultural resistance to regulation all ensure that any chilling effect of these export restrictions will be *de minimis*.

---

53. *See* John Markoff, *Federal Inquiry on Software Examines Privacy Programs*, N.Y. TIMES, Sept. 21, 1993, at D1.

54. *See* Arms Export Control Act, *supra* note 30; *New S.P.A. Study: Export Regulations Preclude U.S. Companies from a Cashing in on Multi-million Dollar Encryption Software Market*, BUS. WIRE, Sept. 1, 1993, *available in* LEXIS, News Library, Curnws file [hereinafter *S.P.A. Study*].

55. *S.P.A. Study*, *supra* note 54.

56. *See generally Federal Inquiry on Software Examines Privacy Programs*, N.Y. TIMES, Sept. 21, 1993, at D1.

A. *The First Amendment*[57]

Not only is the current regime of data classification and regulation probably constitutionally unproblematic, but the general policy objections to U.S. government control seem unpersuasive because government overreaching is rare and national security is a legitimate goal. Scientific expression enjoys protection against content-based prior restraint under the First Amendment. The case of *Near v. Minnesota*[58] outlines the limited exceptions in which the government may make a prior restraint on speech. These are restraints on obstructions to military recruiting, publication of troop numbers and movements, obscene materials, and incitements to violence or forcible overthrow of the government.

The Atomic Energy Act (AEA) is the only federal statute explicitly authorizing a prior restraint on dissemination of scientific research insofar as information about atomic energy and weapons is "born classified."[59] This was the statutory basis of the United States entering federal court seeking an injunction against the publication of the Progressive Magazine. Part of the court's reasoning in granting a preliminary injunction against that publication was its belief that information on nuclear weapons is like information on troop movements. It is not clear how persuasive this reasoning would be had that case had full procedural review. It is easy to imagine that portion of the AEA authorizing injunction against publication being struck down on its face if a higher court disagreed that a weapons system resembles a group of soldiers to the extent that it too would fall under a prior restraint exception in *Near*.[60] Moreover, there has been only one other court challenge to the national security classification of privately generated data, which suggests that the administrators of the AEA have been circumspect in how broadly they will interpret the act.[61]

Export restrictions as well are constitutionally sound, as they contemplate a licensing scheme administered on a case-by-case basis and are probably a time, place, or manner restriction. For example, even unclassified data subject to the strictest licensing restrictions can ordinarily be shared with another U.S. citizen. National security is a constitutionally valid government interest, and overreaching in practice

---

57. *See generally* Harold P. Green, *Constitutional Implications of Federal Restrictions on Scientific Research and Communication*, 60 U.M.K.C.L. REV. 619 (1992).

58. 283 U.S. 697 (1931).

59. *See* Green, *supra* note 57, at 630.

60. *See id.* at 637.

61. *See id.* at 632–33.

seems rare, as licensing regulations contain assurances of due process in review procedures.

Additionally, much science falls under U.S. government contract, and few can object that the U.S. government has a proprietary interest in the results of such research for enforcing the contractual provisions that restrict their communication.[62] The SPIE case, in which contractual terms within the funding grants authorized DOD restrictions, stands out more as an anecdote of bureaucratic befuddlement than as a symptom of systematic censorship. The vigor of the United States' enforcement of these contractual provisions has varied under different administrations and different circumstances, but their validity as controls over government "property" is even less subject to constitutional challenge than is the case of classification of privately generated information.[63] Moreover, governmental control over funding itself appears to have more of an influence over what academic science gets done than enforcement of export regulations. The First Amendment remains a sound barrier protecting scientists from illegitimate government encroachment on their endeavor.

B. *The Internet*

Another factor protecting fundamental research in addition to special treatment under the export regulations is the access most U.S. scientists have to the Internet global computer network. They can transmit data to colleagues worldwide almost instantaneously. Originally a project of the DOD Advanced Research Projects Administration, the Internet has grown from a military logistics and supply tool linking a few military bases to an immense web of research institutions, corporations, military, and other organizations. Estimates on its current number of users vary from about 10 million to over 20 million, with a growth rate estimated at around 10% more new users every month.[64] Any computer data file can be transmitted to any other person on the network in a very short time, depending only on the file's size. The U.S. government, cable companies, and telephone companies have all expressed a commitment to enlarge the Internet user base, improve its "backbone" to allow even faster transmission speeds, and expose a greater diversity of people to the social and educational benefits of the

62. *See id.* at 628.

63. *Id.* at 628–29.

64. *See* John Burgess, *Data Highways . . . Can We Get There From Here?*, WASH. POST, May 2, 1993, at H1, H7.

network.[65] The current academic and "cyberpunk" culture of Internet users is evolving, unwillingly in some cases, to fit the new commercial and educational role that the network will soon have.[66]

Eavesdropping on extraterritorial transmissions, the NSA's mandate, will clearly become more difficult if only because of the increasing volume and size of transmissions.[67] Any enforcement capability that it has right now over preventing illegal transmissions of scientific data may soon be whittled away, especially if private groups are successful in creating encryptions that the NSA cannot break, or at least not without difficulty. This, according to some, explains the U.S. government's zealousness in prosecuting criminal cases which may involve groups capable of compromising the NSA's tenuous ability to maintain oversight over data communications.[68]

There is an irony in that the medium seems to have spawned its own protections from U.S. government control, thereby prodding the federal government to enforce the controls it still has. In the case of P.G.P., the program apparently traveled the world via the Internet. Likewise, DES has been transmitted to restricted areas over the Internet. In this respect, regulations that prevent the export of any information, classified or unclassified, private or government sponsored, seem outmoded to the degree that violations cannot be policed.

C. *The Norms of Science*

Like the cyberpunks' neo-libertarian aversion to any commercialization or regulation of the Internet, scientists' values in favor of free and open communication of scientific results will serve as a check on government abridgment of academic freedom. Cultural norms are commonly attributed to scientists who pursue the goal of the "extension of certified knowledge."[69] The freedom to communicate results is a value that rests on the norms within the scientific community of "universalism, communism [sic], disinterestedness, and organized skepticism."[70] Without the

---

65. *See id.* at H1; *Data Communications Program Charted Future Information Highway*, 87 A.B.A. SEC. SCI. & TECH. 9 (1993); Tim Studt, *Can High Performance Networks Meet Future R & D Needs: Network Technology For Research and Development*, R & D, Oct. 1992, at 30.

66. *See generally Cyberpunk!*, *supra* note 49.

67. *See Spy Vs. Computer Nerd: The Fight over Data Security*, *supra* note 52, at 43.

68. *See id.*

69. *See* Rebecca S. Eisenberg, *Proprietary Rights and the Norms of Science in Biotechnology Research*, 97 YALE L.J. 177, 183 (1987), (quoting R. MERTON, *The Normative Structure of Science*, in THE SOCIOLOGY OF SCIENCE at 267 (1973)).

70. *Id.*

freedom of a scientist to expose his or her peers to the results of research, the program of extending knowledge could become weakened because these norms could not be followed. Other scientists would not be able to verify results by replicating research, experimental design could not be reviewed with other experts in a particular field to iron out bugs, a culture of suspicion might replace a culture of openness, and subsequent empirical testing could not build upon results.

Nevertheless, aside from the case of the AEA (which might ultimately not pass a constitutional review), restrictions on private academic science do not in principle exist. Export regulations under the EAA do not touch upon "fundamental research" performed by private actors. In fact, those regulations affect only research that is the performed with a proprietary interest in mind. Restrictions on communications regarding such research arguably do not clash with the norms of science at all because proprietary science is usually secret anyway.[71] The U.S. government does have a legitimate proprietary interest in research performed under government contract, and President Reagan's 1985 directive on scientific research proclaims that the products of "fundamental research" even under U.S. governmental control should not be classified, to the extent nonclassification is possible. This introduces some element of discretion in the control of such research, but it has only been in the last decade that real opposition to classification in the abstract has been voiced by scientists.[72] This leads one to wonder how scientists felt about classification in the first thirty years that it was a common U.S. government method of control over communication of U.S. sponsored research results.[73]

It is possible that in the last ten years the federal government has been more vigorous than in the previous thirty years in enforcing its proprietary rights over research results. If this is true, then scientists will let the government know in which circumstances it has crossed a line in opposition to the norms of science in a way damaging to the extension and certification of knowledge. The DOD classification review at the SPIE was considered anomalous in the scientific community, and became the focus of outrage for many years afterward.[74] President Reagan's 1985 directive on scientific research was issued in response to the concerns by scientists that fundamental research would be threatened

71. *See generally* Eisenberg, *supra* note 69.
72. *See* Green, *supra* note 57, at 642.
73. *See id.*
74. *See* Ramirez, *supra* note 42, at 191.

under the current classification regime.[75] The uncooperativeness of university professors and administrators with the Department of State in enforcing visa restrictions also points to circumstances of scientists holding their ground in support of their institutional norms. The Internet is a simple and fast means of "civil disobedience" to those scientists who feel morally compelled to resist regulations which they believe oppose their fundamental project, as the writer of P.G.P. might have done.[76] The norms of science ensure that academic freedom will remain largely untouched by any regulatory scheme that is constitutionally valid.

CONCLUSION

The federal government has several means to the control of technical data in the form of scientific research results. These include security classification and export regulation under the EAA. While some may object that these controls are wrong in principle, this is probably not the case because national security is a legitimate government end. While others might object that these controls are wrong as applied, this too is probably not the case because constitutional protections, the ease with which scientists may disobey the controls, and attitudes of scientists compelling them to voice concern when it is necessary all suggest that overreaching by the government would be rare and incapable of greatly diverting the progress of the scientific endeavor.

75. *See* Swan, *supra* note 10, at 617–23.

76. Carey, *supra* note 52, at 43.