Oral Argument Scheduled For December 8, 1997

In The
UNITED STATES COURT OF APPEALS
For The Ninth Circuit

No. 97-16686
C-95-0582 MHP (N.D. California, San Francisco)

Daniel J. Bernstein,

Plaintiff/Appellee,

v.

United States Department of Commerce, et. al.,

Defendants/Appellants

Appeal from the United States District Court
for the Northern District of California

BRIEF FOR AMICI CURIAE

ELECTRONIC PRIVACY INFORMATION CENTER; AMERICAN CIVIL LIBERTIES UNION; AMERCIAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA; CENTER FOR DEMOCRACY AND TECHNOLOGY; COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY; ECONOMIC STRATEGY INSTITUTE; FREE CONGRESS RESEARCH AND EDUCATION FOUNDATION; HUMAN RIGHTS WATCH; INDEPENDENCE INSTITUTE; INTERNATIONAL INFORMATION SYSTEM SECURITY CERTIFICATION CONSORTIUM; INTERNET MAIL CONSORTIUM; INTERNET SOCIETY; NATIONAL ASSOCIATION OF MANUFACTURERS; PRIVACY INTERNATIONAL; U.S. PUBLIC POLICY COMMITTEE OF THEH ASSOCIATION FOR COMPUTING; DR. WHITFIELD DIFFIE; DR. PETER NEUMANN; and DR. RONALD RIVEST

Marc Rotenberg
David L. Sobel
ELECTRONIC PRIVACY
INFORMATION CENTER
666 Pennsylvania Ave., S.E.
Washington, DC 20003
(202) 544-9240

Ivan K. Fong
Dawn C. Nunziato
David W. Addis
COVINGTON & BURLING
1201 Pennsylvania Ave., N.W.
Washington, DC 20044-7566
(202) 662-6000

Counsel for Amici Curiae

November 7, 1997

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

A. Parties and Amici.

A motion for leave to participate as amici curiae and to join this brief was filed in this Court on behalf of all amici listed on this brief. The parties have consented to such participation.

B. Rulings Under Review.

References to the rulings at issue appear in the Brief of Appellee.

INTERESTS OF THE AMICI CURIAE

The Electronic Privacy Information Center ("EPIC") is a non-profit, public interest research center whose mission is to focus public attention on emerging civil liberties issues in the field of electronic information. EPIC is sponsored by the Fund for Constitutional Government, a non-profit organization established in 1974 to protect privacy, the First Amendment, and other constitutional rights. EPIC monitors and disseminates information about court decisions and government policies that affect electronic privacy. EPIC has developed an expertise in the legal issues in this area, as well as a technical expertise in encryption that helps to illuminate the practical aspects of the issues currently before the Court.

The American Civil Liberties Union ("ACLU") is a nationwide, non-partisan organization of nearly 300,000 members dedicated to defending the principles of liberty and equality embodied in the Bill of Rights. Throughout its 75-year history, the ACLU has been particularly concerned with abridgements of the freedoms guaranteed by the First Amendment. The ACLU has worked to ensure that First Amendment protections are extended to each new communications technology -- telephone, radio, television, cable, and now on-line communications. The ACLU has appeared before the Supreme Court and the Courts of Appeals in numerous cases involving the First Amendment, both as direct counsel and as amicus curiae.

The ACLU of Northern California is a regional office of the national ACLU and has been an active litigant in this Court on issues concerning freedom of expression.

The Center for Democracy and Technology ("CDT") is an independent, non-profit, public interest organization in Washington, D.C. CDT's mission is to develop and implement public policies to protect and advance individual liberty and democratic values in new digital communications media. CDT has been deeply involved in the ongoing public debate over national and international encryption policies, including recent publication of the widely-cited experts' study on The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption. CDT believes that the freedom to use and distribute encryption technologies is essential to the protection of individual privacy and free expression in the emerging global information infrastructure.

Computer Professionals for Social Responsibility ("CPSR") is a national alliance of computer scientists and others concerned about the impact of computer technology on society. CPSR members provide policymakers and the public at large with realistic assessments of the power, promise, and limitations of computer technology. CPSR is concerned with the impact of computing technology and personal privacy. CPSR is concerned that legal barriers to the dissemination of encryption technology are detrimental to the development of electronic commerce and the ability to participate in this rapidly growing global opportunity.

The Economic Strategy Institute ("ESI") is a non-profit research center founded in 1989 to develop and promote a comprehensive strategy for American economic leadership in the 21st century. It is funded by a combination of corporate, individual, and foundation grants. ESI believes that the development of the world's most advanced and secure telecommunications networks is vital to our future. ESI recognizes that maintaining a cutting-edge cryptography industry in the United States is important for national security and economic reasons and that electronic commerce, the Internet, and other advanced communications networks will likely be the economic growth engine for the United States in the next century.

The Free Congress Research and Education Foundation ("the Foundation") was founded in 1977 as a non-partisan, non-profit, tax-exempt research and education foundation dedicated to conservative governance, traditional values, and institutional reform. The Foundation's research, education, and training programs prepare and support conservative leaders and activists in the Nation's capital, throughout the United States, and around the world. The Foundation most recently has engaged in a number of projects related to the protection of personal privacy with respect to advancing technologies and the role they play in that area.

Human Rights Watch ("HRW") is a non-profit organization that investigates and reports violations of human rights in over 70 countries worldwide. As a public advocate of the international right of free expression, it defends the use of encryption as a form of speech and a means to protect whistle-blowers, human rights advocates, and victims of human rights abuse from government reprisals. HRW uses encryption to communicate with human rights activists around the globe and participates in conferences and training courses designed to familiarize local human rights activists with encryption.

The Independence Institute (the "Institute") is a non-profit public policy research organization, dedicated to the limited-government, individual-responsibility principles of the Declaration of Independence. Located in Golden, Colorado, the Institute seeks to promote civil liberty and constitutional rights in a wide variety of contexts. The Institute has presented testimony to Congress, written newspaper opinion pieces, and authored scholarly journal articles in favor of open access to strong cryptography. The Institute's ability to provide information to, and communicate with, its domestic and foreign website users can be enhanced by the ability of users to send messages to and receive messages from the Institute using strong cryptography.

The International Information System Security Certification Consortium ("ISC2") is a group of some 900 certified information system security professionals ("CISSPs") in the United States and abroad. CISSPs are bound by the ISC2 Code of Ethics, one of which is to support efforts to promote the understanding and acceptance of prudent information security measures throughout the public, private, and academic sectors of our global information society. ISC2 is incorporated as a not-for-profit corporation in the Commonwealth of Massachusetts.

The Internet Mail Consortium ("IMC") is an industry association of vendors of Internet mail software and services. IMC's members include large and small software companies, Internet service providers, and end users of Internet mail. Internet mail relies on cryptography for authentication and privacy, and IMC's members desire a wide unfettered market for secure Internet mail products.

The Internet Society ("ISOC") is a non-governmental international organization for worldwide coordination and collaboration of Internet issues, standards, and applications. ISOC has over 7,500 members, currently representing over 150 countries of the world and comprised of commercial companies, governmental agencies, foundations, and individuals. ISOC serves to assure the beneficial, open evolution of the global Internet and its related internetworking technologies.

The National Association of Manufacturers ("the NAM") is the Nation's oldest and largest broad-based industrial trade association. Its more than 14,000 member companies and subsidiaries, including 10,000 small manufacturers, employ approximately 85 percent of all manufacturing workers and produce over 80 percent of the Nation's manufactured goods. More than 158,000 additional businesses are affiliated with the NAM through its Associations Council and National Industrial Council.

Privacy International ("PI") is an international human rights group formed in 1990 to monitor surveillance by governments and corporations. PI promotes the use of laws and technology to improve personal privacy. It is based in London, U.K. with offices in Washington, D.C. and Sydney, Australia and has members in more than 40 countries.

The U.S. Public Policy Committee of the Association for Computing serves as the focal point for the interaction by the Association for Computing ("ACM") with U.S. government organizations, the computing community, and the U.S. public in all matters of U.S. public policy related to information technology. ACM, chartered in 1947, is an 80,000-member, non-profit, tax-exempt, international scientific and educational organization dedicated to advancing the art, science, engineering, and application of information technology.

Dr. Whitfield Diffie holds the position of Distinguished Engineer at Sun Microsystems. In 1992, he was awarded a Doctorate in Technical Sciences (Honoris Causa) by the Swiss Federal Institute of Technology for his 1975 discovery of the concept of public key cryptography. Dr. Diffie served on the ACM cryptography study panel, frequently testifies before Congress on encryption policy issues, and is the co-author (with Susan Landau) of the forthcoming book, Privacy on the Line: The Politics of Wiretapping and Encryption. He is a co-founder of the International Association for Cryptologic Research and the recipient of the IEEE Information Theory

Society Best Paper Award for 1979 and the IEEE Donald E. Fink Award for 1981.

Dr. Peter Neumann served on the ACM and National Research Council ("NRC") cryptography studies and on the NRC Computers at Risk study. He has long been involved in research in security, reliability, safety, and system risks. He is Principal Scientist in the Computer Science Laboratory at SRI International. He is a Fellow of the American Association for the Advancement of Science, the ACM, and the Institute of Electrical and Electronics Engineers.

Dr. Ronald Rivest is the Webster Professor of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology, an associate director of MIT's Laboratory for Computer Science, and a leader of that lab's Cryptography and Information Security research group. He is a Fellow of the ACM and of the American Academy of Arts and Sciences and is also a member of the National Academy of Engineering. Dr. Rivest is an inventor of the RSA Public Key Cryptosystem, a founder and director of RSA Data Security, and has served as a director of the International Association for Cryptologic Research.

STATEMENT OF JURISDICTION

Amici agree with Appellant's statement of jurisdiction.

STATUTES AND REGULATIONS

The pertinent statutes and regulations are attached to the Brief of Appellant.

STATEMENT OF THE CASE

This case is a constitutional challenge to certain U.S. government export regulations that restrict the publication and dissemination of encryption software and related technical information. Originally embodied in the Arms Export Control Act, 22 U.S.C. " 2751-2796d (1997) and the International Traffic in Arms Regulations ("ITAR"), 22 C.F.R. pts. 120-30, these regulations are now embodied, with essentially identical restrictions, in the Export Administration Regulations, 15 C.F.R. pts. 730-74.

I. The Present Litigation

Appellee Daniel Bernstein is a computer science professor at the University of Illinois. While a Ph.D. candidate in the Mathematics Department at the University of California at Berkeley, he developed a mathematical algorithm useful for encrypting information. His creation, which he entitled "Snuffle," was expressed in a scientific paper and as "source code" written in a high-level programming language called C. Professor Bernstein sought to publish both the Snuffle source code and related information about Snuffle through the ordinary channels of scientific interchange, including the Internet and at conferences, for evaluation, testing, and critique by the world-wide scientific and software publishing communities.

In 1992, Professor Bernstein filed a commodity jurisdiction request with the State Department to determine whether the Snuffle source code or the related information was controlled by the ITAR. In 1992 and 1993, the State Department asserted that the Snuffle source code, the scientific paper, and all other Snuffle technical information, were controlled by the ITAR./ The ITAR required the State Department to approve (in the form of a license) the export of source code or related information. Without such a license, Professor Bernstein was prohibited from, among other things, posting the information on the Internet using a computer in the United States or disclosing the information to foreign nationals in the United States (except in limited circumstances).

Professor Bernstein filed this action in 1995 in the District Court for the Northern District of California, arguing, inter alia, that the ITAR's restrictions on encryption software and related technical information violated the First Amendment on their face and as applied to him. The District Court held that encryption source code is speech entitled to First Amendment protection and granted partial summary judgment in favor of Professor Bernstein on his constitutional claim. See Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426 (N.D. Cal. 1996) ("Bernstein I"); Bernstein v. U.S. Dep't of State, 945 F. Supp. 1279 (N.D. Cal. 1996) ("Bernstein II").

In November 1996, President Clinton ordered that jurisdiction over non-military encryption items, including encryption software and related technical information, be transferred from the State Department to the Commerce Department. See E.O. 13026, 61 Fed. Reg. 58,767 (Nov. 19, 1996). In December 1996 -- shortly after the Bernstein II decision -- the Commerce Department adopted amendments to the Export Administration Regulations. The amendments contained restrictions on dissemination of encryption software and related technical information that are, in all respects relevant to Professor Bernstein's claims, essentially identical to the former ITAR restrictions, as the government conceded below.

The District Court then granted partial summary judgment for Professor Bernstein, holding that the Regulations impose a prior restraint on speech in violation of the First Amendment and enjoining the government from enforcing the new EAR encryption regulations. See Bernstein v. U.S. Dep't of State, No. C-95-0582, 1997 U.S. Dist. LEXIS 13146 (N.D. Cal. Aug. 25, 1997) ("Bernstein III").

II. The Export Administration Regulations on Encryption

The Export Administration Regulations ("Regulations" or "EAR") set forth comprehensive controls on exports of non-military commodities and information from the United States./ The Regulations divide the export control regime into two mutually exclusive categories, "commodities" and "technology," and treat software as a form of "technology" -- i.e., information or know-how -- and not as a commodity. See 15 C.F.R. pt. 772; see also 50 U.S.C. App. " 2415(3), (4).

The December 1996 amendments to the Regulations create a new set of strict "EI controls" for "encryption items," defined as "all encryption commodities, software, and technology that contain encryption features and are subject to the EAR." 15 C.F.R. pt. 772. EI-controlled encryption software and technology cannot be exported (except to Canada) without applying for and receiving an individual license from the Commerce Department. See 15 C.F.R. " 736.2(b), 742.15(a).

"Export" is defined expansively under the Regulations to include not only "actual shipment or transmission . . . out of the United States" or "release of technology or software in a foreign country" -- the conventional meaning of "export" -- but also transfers or disclosures that take place entirely within the United States: (1) For encryption software, including source code, "export" includes making the software available on Internet sites or any other "communications facilities" accessible to persons outside the United States, unless certain onerous precautions are taken, 15 C.F.R. ' 734.2(b)(9)(ii); and (2) for other kinds of encryption technical information, "export" includes "any release of technology" -- including "visual inspection" or "oral exchanges of information" -- to a foreign national within the United States (other than a permanent resident or qualifying refugee), 15 C.F.R. " 734.2(b)(2), (3).

Thus, if a publication or distribution qualifies as an "export" under one of these broad definitions, and unless an exception applies,/ a pre-publication license from the Commerce Department is required before publishing or distributing encryption source code or technical information outside or within the United States.

Where a pre-publication license is required, the discretion of the government to grant or deny the license is essentially unbounded. The Regulations provide only that "applications will be reviewed on a case-by-case basis" by the Commerce Department, in conjunction with several other agencies, to determine whether the export or re-export "is consistent with U.S. national security and foreign policy interests." 15 C.F.R. " 742.15(b), 750.3(b). No definite time for a final decision is established, and judicial review is apparently unavailable. See 15 C.F.R. " 756.2(c).

SUMMARY OF ARGUMENT

Text expressed in a computer programming language is an important medium of communication of scientific theories and ideas among scientists and is therefore protected under the First Amendment. The government's post hoc characterization of cryptographic source code as a "product" as opposed to "information" does not insulate such text from First Amendment protection. By requiring a government-issued license prior to the publication or dissemination of cryptographic source code, the Export Administration Regulations impose a prior restraint on protected expression. Because the government's licensing determination under the Regulations is standardless and discretionary, and because the EAR-imposed prior restraint fails to provide necessary procedural safeguards, the Regulations embody an unconstitutional prior restraint on protected expression.

The Regulations also constitute a content-based restriction on protected expression that is not narrowly tailored to serve a compelling government interest. Even assuming arguendo that the Regulations were content-neutral restrictions on expression, they would not withstand intermediate constitutional scrutiny because they are not narrowly tailored to serve the

government's asserted national security ends.
Furthermore, the Regulations burden private speech by burdening the tools necessary to achieve communications privacy in the electronic sphere. By restricting the use of cryptographic software, the Regulations thwart individuals' reasonable expectations of privacy in their electronic communications.

STATEMENT ON CRYPTOGRAPHY

I. Cryptography and the protections to privacy interests it provides are vital components of emerging global communications technologies.

Emerging computer and communications technologies are radically altering the ways in which we communicate and exchange information. Along with the speed, efficiency, and cost-saving benefits of the "digital revolution" come new challenges to the security and privacy of communications and information traversing the global communications infrastructure. As one commentator has observed, "the ease with which electronic mail messages can be intercepted by third parties means that communicating by public electronic mail systems, like the Internet, is becoming almost as insecure as talking in a crowded restaurant." A. Michael Froomkin, The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution, 143 U. Pa. L. Rev. 709, 724 (1995) (footnote omitted). As the National Research Council's Committee to Study Cryptography Policy ("NRC Committee") noted last year, the threat to personal privacy is substantial:

> Increasing reliance on electronic commerce and the use of networked communication for all manner of activities suggest that more information about more people will be stored in network-accessible systems and will be communicated more broadly and more often, thus raising questions about the security of that information.

National Research Council, Cryptography's Role in Securing the Information Society ' 1.5, at 41 (1996) ("NRC Report"). Likewise, in a 1993 report to Congress, the General Accounting Office warned that "[t]he increased use of computer and communications systems by industry has increased the risk of theft of proprietary information." GAO, Communications Privacy -- Federal Policy and Actions, No. GAO/OSI-94-2, app. Sec. I:1 (1993) ("Communications Privacy").

In response to these challenges, the mechanisms that secured traditional paper-based communications -- envelopes and locked filing cabinets -- are being replaced by cryptographic security techniques. Through the use of cryptography, communications and information stored and transmitted by computers can be protected against interception. With the advent of the computer revolution and recent innovations in the science of encryption, a new market for cryptographic products has developed. Electronic communications are now widely used in the civilian sector and have become an integral component of the global economy. Computers store and exchange an ever-increasing amount of highly personal information, including medical and financial data. In this electronic environment, the need for privacy-enhancing technologies is apparent. See, e.g., David Chaum, Achieving Electronic Privacy, Scientific American, Aug. 1992, at 96. Communications applications such as electronic mail and electronic fund transfers require secure means of encryption and authentication -- features that can only be provided if cryptographic technology is widely available and unencumbered by government regulation.

Although the technical details of cryptographic systems are quite complex, the underlying concepts can be easily grasped. Cryptography provides a means of accomplishing two crucial functions -- encryption and authentication. Encryption is the process of encoding or "scrambling" the contents of any data or voice communication with an algorithm (a mathematical formula) and a randomly selected variable associated with the algorithm, known as a "key." Only the intended recipient of the communication, who holds the key, can decrypt and access the information. The key is essentially a string of numbers; the longer the string, the stronger the security.

The authentication capabilities of cryptographic systems involve the use of "digital signatures." A digital signature is a cryptographically-based assurance that a particular document was created or transmitted by a given person. See generally ABA Science & Technology Section, Digital Signature Guidelines (1996). It thus provides a means of authenticating the integrity of electronically transmitted data and the identity of the sender, much as a handwritten signature verifies the authenticity of a paper record. Digital signatures also provide for the "non-repudiation" of electronic data -- the inability to deny the authenticity of the transmitted information. As we move toward increased reliance on electronic communications, the importance of such capabilities is apparent.

A. Cryptography is a prerequisite for electronic commerce; export controls impede its development both domestically and globally.

Cryptographic technology is an essential component of the secure communications infrastructure required for meaningful electronic commerce and continued economic development. In a study commissioned by the Business Software Alliance, a leading group of computer scientists and cryptography scholars concluded that:

> Encryption plays an essential role in protecting the privacy of electronic information against threats from a variety of potential attackers. . . .The dirt paths of the middle ages only became highways of business and culture after the security of travelers and the merchandise they carried could be assured. So too the information superhighway will be an ill-traveled road unless information, the goods of the Information Age, can be moved, stored, bought, and sold securely.

Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security, (visited October 27, 1997) (attached at Appendix A).// Likewise, the Internet Architecture Board ("IAB") and the Internet Engineering Steering Group ("IESG"), the bodies that oversee architecture and standards for the Internet, recently observed that:

> [a]s more and more companies connect to the Internet, and as more and more commerce takes place there, security is becoming more and more critical. Cryptography is the most powerful single tool that users can use to secure the Internet. Knowingly making that tool

> weaker threatens their ability to do so, and has no proven benefit.

IAB and IESG Statement on Cryptographic Technology and the Internet 4 (July 24, 1996) ("IAB and IESG Statement") (attached at Appendix A).

Governmental restrictions on the export of encryption software -- and the draconian manner in which they are applied -- impede the development of the secure global infrastructure that electronic commerce requires. Less apparent is the effect of these restrictions on the domestic development and use of privacy-enhancing cryptographic technologies, to the detriment of individual rights and commercial concerns within the United States. This domestic impact occurs as a result of the global nature of computer technology and networked communications. A global communications infrastructure requires "interoperability" -- the ability of a user in the United States to communicate with a European user through systems that employ common technological standards. In the context of encryption technology, this requires information to be encrypted and/or authenticated using the same cryptographic system. If a user outside of the United States cannot decrypt a message encrypted by a system that may legally be sold only in the United States, the functionality and marketability of that system is substantially limited.

The problem of interoperability, coupled with U.S. export restrictions on encryption software, has led many U.S. software manufacturers to produce relatively weak security products that can be sold both at home and abroad. This is particularly true of "integrated" products, such as word processing and spreadsheet programs that contain cryptographic capabilities. As the NRC Committee found,

> U.S. export controls have had a negative impact on the cryptographic strength of many integrated products with encryption capabilities available in the United States. Export controls tend to drive major vendors to a "least common denominator" cryptographic solution that will pass export review as well as sell in the United States. . . . Export controls distort the global market for cryptography . . . .

NRC Report, supra, ' 4.3.1, at 138 (footnote omitted).

For more than a quarter of a century, the United States has led the world in the development of computer and communications technology. That leadership position is now being threatened by the controls on cryptography at issue in this case./ As noted, a global communications infrastructure has emerged (largely as a result of U.S. innovation), requiring sophisticated techniques for the security and privacy of communications. Individuals will increasingly demand that their personal privacy be preserved in the new information environment, and commercial entities will require the highest level of protection for valuable financial and proprietary data.

For example, restrictions on the use of encryption technology render it more difficult for U.S. companies to protect their valuable trade secrets against industrial espionage. Many U.S. companies now use software files -- instead of blueprints or other paper-based means of storage -- to store their secret product designs./ Strong encryption is an important means of protecting such product designs. The trade secrets of U.S. companies have come under increasing attack not only by U.S. competitors but also by foreign governments themselves./ Although Congress recently enacted the first-ever federal trade secret law in the Economic Espionage Act (P.L. 104-294, 110 Stat. 3488 (1996)) to help prevent such industrial espionage, the far preferable method of preserving U.S. companies' trade secrets is through the use of strong encryption to protect such secrets before they are misappropriated.

Future leadership in the field of information technology will depend upon leadership in the field of information security. The demand for security must be met, if not by U.S. engineers and software developers, then by their foreign competitors. Although controls on the export of encryption software are asserted to be necessary for national security, "[t]he development of foreign competitors in the information technology industry could have a number of disadvantageous consequences from the standpoint of U.S. national security interests." NRC Report, supra, ' 4.4.2, at 156.

In sum, the export restrictions on encryption software at issue in this case have had, and will continue to have, a substantial detrimental effect on the U.S. computer, communications, and other industries. Because these export restrictions require U.S. software manufacturers to market only products with weak and insufficient security features, the restrictions hobble U.S. software manufacturers and severely endanger their future world leadership. The export restrictions also endanger U.S. national security interests by allowing foreign encryption technology to flourish, while stunting the development of U.S. encryption technology.

B. Restrictions on the dissemination of cryptographic information infringe upon individual privacy rights.

Governmental regulation of the free flow of information concerning cryptographic security techniques endangers personal privacy as well as commerce. As the recent IAB and IESG Statement noted, oversight bodies "are concerned by the need for increased protection of international commercial transactions on the Internet, and by the need to offer all Internet users an adequate degree of privacy." IAB and IESG Statement, supra, at 1. Indeed, cryptographic technology is becoming an increasingly vital tool for human rights activists, political dissidents, and whistle-blowers throughout the world to facilitate confidential communications free from intrusion. For example, amicus Human Rights Watch increasingly uses encryption in its communications with human rights activists around the globe. Its Hong Kong office has routinely encrypted communications since the July 1997 transfer of sovereignty over the territory to the People's Republic of China, a government that has punished peaceful expression of human rights criticism as counterrevolutionary crime. See also David Banisar, A Primer on Electronic Surveillance for Human Rights Organizations, International Privacy Bulletin (July 1993).

Cryptographic techniques can also provide confidentiality of electronic mail and personal records, such as medical information and financial data, which are increasingly at risk of theft or misuse when stored in a networked environment. Indeed, two decades ago the Supreme Court recognized the risks

to personal privacy created by unwarranted disclosures of information maintained by the government itself:
We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files . . . . much of which is personal in character and potentially embarrassing or harmful if disclosed.

Whalen v. Roe, 429 U.S. 589, 605 (1977) (footnote omitted). These risks have increased substantially as virtually all vital records, both public and private, are now maintained electronically, many of which are stored in networked environments with insufficient security.

In short, the governmental regulations at issue not only hobble the development of electronic commerce, but jeopardize personal privacy interests as well.

ARGUMENT

I. The text at issue is itself protected expression under the First Amendment.

A. The First Amendment protects a broad range of scientific and artistic expression, including text expressed in computer programming languages.

To communicate his ideas and theories on cryptography to other scientists, Professor Bernstein sought and was refused a governmental determination that text written in C programming language could be freely disseminated. The District Court correctly determined that the software at issue constitutes speech for purposes of First Amendment analysis. See Bernstein I, 922 F. Supp. at 1436; Bernstein II, 945 F. Supp. at 1287; see also Karn v. U.S. Dep't of State, 925 F. Supp. 1, 9-10 (D.D.C. 1996) (holding that First Amendment protection extends to encryption source code and embedded comments), remanded, 107 F.3d 923 (D.C. Cir. 1997); United States v. Mendelsohn, 896 F.2d 1183, 1186 (9th Cir. 1990) (recognizing that computer programs may warrant First Amendment protection). This Court should uphold the District Court's determination that software is expression protected by the First Amendment.

The First Amendment protects a broad range of scientific and artistic expression. To be worthy of First Amendment protection, expression need only be a vehicle for the communication of thoughts, ideas, opinions, or emotions. Expression is protected if, given the context or environment in which it is undertaken, it contains sufficient communicative elements. See Spence v. Washington, 418 U.S. 405 (1974). As leading First Amendment scholar Thomas Emerson explained in discussing the role of free expression in a democratic society,

> [E]very man -- in the development of his own personality -- has the right to form his own beliefs and opinions. And, it also follows, that he has the right to express these beliefs and opinions. Otherwise they are of little account. For expression is an integral part of the development of ideas, of mental exploration and of the affirmation of self. . . . Hence, suppression of . . . expression is an affront to the dignity of

> man, a negation of man's essential nature. . . . From these concepts there follows the right of the individual to access knowledge; to shape his own views . . .; in short, to participate in formulating the aims and achievements of his society and his state.

[T]hought and communication are the fountainhead of all expression of the individual personality. To cut off the flow at the source is to dry up the whole stream. Freedom at this point is essential to all other freedoms.

Thomas I. Emerson, Toward a General Theory of the First Amendment, 72 Yale L.J. 877, 879-81 (1963).

The purview of the First Amendment encompasses a wide variety of scientific and artistic speech. Included within the First Amendment's sphere of protection are, for example, the abstract paintings of Jackson Pollack, the esoteric classical music of Arnold Schönberg, rock music, modern dance, and the nonsense verse of Lewis Carroll. See Hurley v. Irish-American Gay, Lesbian and Bisexual Group, 515 U.S. 557, 569 (1995); Ward v. Rock Against Racism, 491 U.S. 781 (1989). To be granted First Amendment protection, expression need not be communicative to all members of a community or be meaningful to a general audience; rather, protected expression may serve as a vehicle of communication only among specialized communities (such as esoteric classical music, experimental theater, abstract art, or abstruse scientific speech, each of which is meaningful only to certain subsets of society). Scientific expression, no less than artistic expression, falls squarely within the rubric of First Amendment protection. See Miller v. California, 413 U.S. 15 (1973) (works with scientific, artistic, political, or literary value protected by First Amendment).

Expression does not forfeit its First Amendment protection merely because it interacts or may interact with a machine. Motion pictures, recorded music, books on tape or on CD-ROM, and text on the Internet are all protected by the First Amendment regardless of the fact that they cannot be read, heard, or perceived by humans without the aid of a device. See Freedman v. Maryland, 380 U.S. 51 (1965); Reno v. ACLU, 117 S. Ct. 2329 (1997). Similarly, source code is not rendered outside the protection of the First Amendment simply because it may interact with a computer.

Moreover, the fact that source code is stored in electronic form, instead of on paper or some other traditional medium of expression, does not render it unprotected by the First Amendment. On the contrary, throughout this century the First Amendment gradually has been extended to encompass expression via new media, to the point where today, "[t]o an increasing degree, the more significant interchanges of ideas [occur] in electronic media." Denver Area Educ. Telecomm. Consortium, Inc. v. FCC, 116 S. Ct. 2374, 2414 (1996) (Kennedy, J., joined by Ginsburg, J., concurring in part, concurring in judgment in part, and dissenting in part). It is undisputed that the First Amendment applies to expression communicated via new technologies such as the Internet. See, e.g., Reno v. ACLU, supra. Thus, notwithstanding the fact that the text at issue is stored in electronic form instead of on paper, it nonetheless constitutes protected expression under the First Amendment.

Furthermore, expression that may be susceptible to bad tendencies or to being subverted for harmful results or that has perceived harmful secondary effects is nonetheless protected by the First Amendment. See Brandenburg v. Ohio, 395 U.S. 444 (1969) (rejecting bad tendency and clear and present danger tests); Renton v. Playtime Theatres, 475 U.S. 41 (1986). Mere recitations by the government that the expression subject to regulation tends to endanger national security interests will not render the regulations constitutional. See New York Times Co. v. United States, 403 U.S. 713 (1971) (per curiam). Similarly, the government's self-serving statements that its motive for enacting the regulations is not to suppress expression cannot save the regulations from a finding of unconstitutionality. See, e.g., Lakewood v. Plain Dealer Publishing, 486 U.S. 750, 764 (1988).

B. Source code is a fundamental vehicle for communication among scientists.

The expression at issue in this case -- source code written in C programming language containing encryption algorithms -- is an important vehicle for communication among scientists and mathematicians of their theories and ideas. Whether or not source code is associated with expression in the mind of the average member of the community (see Brief of Appellant at 40), source code is a commonly-used and fundamental medium of expression among scientists and mathematicians, as described below. Moreover, programming language is a uniquely-suited formal vehicle for the precise communication of complex scientific and mathematical concepts. Thus, it is not merely the case that programming language is expressive; rather, in many instances, such language is the only appropriate vehicle for the communication of precise, complex ideas among scientists and mathematicians.

The fundamental expressive character of source code is best articulated in the words of those who regularly use it as a medium of scientific expression. As computer scientist Carl Ellison explains, "computer languages are used to communicate between human beings . . . . They are the natural and best means of communication of some kinds of ideas, specifically mathematical concepts in the form of algorithms. . . . [A] fundamental and essential use for [computer languages] is for communication between people." Ellison Decl. & 8 (ER 00104-5). Similarly, computer programmer Richard M. Stallman explains

> [a]s an experienced programmer, I often communicate certain of my ideas in computer languages in order to be more precise about them -- just as mathematicians express equations in mathematical notation and composers express music in musical notation. . . . As a computer programmer, I can communicate using computer programming languages, within the range of what they can express, just as I would using human languages.

Stallman Decl. && 3-4 (ER 00190). Computer Science Professor Harold Abelson concurs: "[t]he notion that computer programs are a medium of expression is widespread throughout computer science education. . . . [C]omputer language . . . is a novel formal medium for expressing ideas about methodology." Abelson Decl. & 8 (ER 00066) (internal quotations omitted).

Thus, source code -- such as the encryption source code at issue in this case -- is essentially text written in a "high-level" language, i.e., a form of language syntactically and semantically similar to natural languages such as English or Spanish. See Encyclopedia of Computer Science 962, 1263-64 (Anthony Ralston & Edwin D. Reilly eds. 3d ed. 1995). See generally Marvin Minsky, Semantic Information Processing 1-32 (1980). An essential function of such source code, and of the English-language "comments" embedded in source code, is to facilitate communication between and among scientists: Just as a mathematics text or written music communicates to a specially trained group of readers, a computer program communicates to its own group of readers. When seen in this light, the First Amendment implications of computer programs are no different from those of many other copyrightable texts.

Alfred C. Yen, A First Amendment Perspective on the Idea/Expression Dichotomy and Copyright in a Work's "Total Concept and Feel," 38 Emory L.J. 393, 431 (1989). Accordingly, as the District Court correctly held, for First Amendment purposes, no meaningful difference exists between high-level programming languages, on the one hand, and natural languages like English and Spanish, on the other. All languages, including high-level computer languages, "participate in a complex system of understood meanings within specific communities." Bernstein I, 922 F. Supp. at 1435.

Source code written in a high-level programming language such as C -- the programming language at issue in this case -- shares many features with other forms of expression that receive First Amendment protection. The communicative nature and expressive qualities of source code and its accompanying comments are readily apparent. To understand this point, it is helpful to consider the following text written in C programming language, which might be used in setting up an interactive, politically-oriented site on the Internet:

```
/* Comment: This program sets forth interactive responses
* to users' answers on a politically-oriented web site.
*/

enum { conservative, liberal, radical, unknown }
Political_Profile;

/* (insert code to set Political_Profile here) */

if (Political_Profile == conservative) {
printf("A conservative is a man who has two \
perfectly good legs who, however, has never \
learned to walk forward. --Franklin Delano \ Roosevelt.\n");

} else if (Political_Profile == liberal) {
printf("A liberal is a man who is willing to spend \ someone
else's money. --Carter Glass.\n");

} else if (Political_Profile == radical) {
printf("I never dared to be a radical when young, \
for fear it would make me conservative when old. \
--Robert Frost.\n")};

} else {
```

```
printf("The marvel of all history is the patience \
with which men and women submit to burdens \
unnecessarily laid upon them by their governments. \
-- William E. Borah.\n")'
}
```

The series of C programming language statements set forth above expresses ideas in a formal, structured form. Similarly, the source code at issue in the instant case expresses ideas in a structured form to a specialized audience./ This expression of ideas, whether emanating from an 18th Century printing press or from a 20th Century source code editor, warrants the protection of the First Amendment./

The government suggests that the Export Administration Regulations do not restrict expression because certain encryption information expressed in certain media -- such as ideas about cryptography set forth in books or articles -- may be freely published under the Regulations. See Brief of Appellant at 38. The government fails to credit, however, the averments of computer science professionals themselves, which make clear that English-language expressions of ideas of cryptography are not sufficient vehicles for communicating their scientific and mathematical ideas. Furthermore, the fact that the Regulations do not restrict the publication of information or source code in paper form that is already publicly available does not mean that the Regulations are not speech-restrictive. The right to freely disseminate what is already widely disseminated is inadequate to guarantee scientists' freedom of expression.

For these reasons, this Court should uphold the District Court's determination that source code constitutes protected expression for purposes of First Amendment analysis.

II. The government cannot avoid First Amendment scrutiny by spurious claims that the EAR encryption regulations do not restrain speech.

The government expressly concedes that source code -- including the encryption source code at issue in this case -- "can be read and understood" by people trained in the particular language in which the source code is written. See Brief of Appellant at 7, 27. That concession should end any dispute about whether encryption source code is entitled to First Amendment protection. In its brief, however, the government attempts to escape the inevitable effect of its concession by a sleight-of-hand. The government first asserts that source code is merely a "product," and then asserts that "the EAR requires a license for the export of encryption products, [but] it does not require a license for the public dissemination of cryptographic information." Id. at 20, 29. The implication is that the Regulations do not restrain speech -- "information" -- in any significant way. But this attempt to draw a false distinction between encryption source code and other kinds of encryption information is not only contradicted by the central importance of source code to communication among scientists, it is also flatly contrary to the specific provisions of the Regulations.

A. The Act and Regulations explicitly recognize that source code and other software are forms of information, not mere "products" or "commodities."

The government's sleight-of-hand depends upon introducing a new term ("product") that is not used in either the Export Administration Act or the Regulations, and then giving that term a meaning completely at odds with the Act and the Regulations. The Export Administration Act divides the subjects of its export control regime into two mutually exclusive categories: "goods" and "technology." The Act defines "goods" as "any article, natural or manmade substance, material supply or manufactured product, . . . excluding technical data." 50 U.S.C. App. ' 2415(3) (emphasis added). "Technology" is defined in turn to encompass "information or know-how [tangible or intangible] that can be used to design, produce, manufacture, utilize or reconstruct goods, including computer software and technical data, but not the goods themselves." 50 U.S.C. App. ' 2415(4) (emphasis added).

The Regulations, based on the Act, follow an exactly parallel structure and thus distinguish between mutually exclusive categories of "commodities" and "technology." Indeed, the Regulations expressly define "commodities" to include "[a]ny article, material, or supply except technology and software." 15 C.F.R. pt. 772 (emphasis added). Reflecting that division, software has always been treated under the EAR as a form of technology -- i.e., information or know-how -- and not as a commodity.

This distinction is not merely theoretical or formal: For instance, non-encryption technology and information in all its forms -- including source code, object code, and all other software -- are free from the Regulations' licensing requirements when they become publicly available through certain specifically-defined methods. See 15 C.F.R. ' 734(b)(3). Commodities, by contrast, cannot qualify as publicly available under these exceptions and are thus subject to the Regulations regardless of availability.

Thus, both the Act and the Regulations explicitly recognize that source code and other software, by their very nature, are forms of "information and know-how" that are distinct from "goods" or "commodities." That is completely at odds with the government's post hoc attempts to invent a new regulatory term, "products," that would encompass both commodities and software. The government cannot defend the Regulations on grounds that are simply at odds with the specific provisions of the Regulations themselves.

The government's claim that source code is fundamentally different from blueprints or technical instructions, and thus can be treated as a mere "product," is similarly misconceived. The fact that source code can be read by a machine as well as an informed person cannot obscure the essential fact that source code can be and is read by people and indeed is a preferred vehicle for communication among scientists, programmers, and others. And, once again, the Regulations themselves belie the government's argument, for the Regulations specifically recognize that blueprints, technical instructions, and software are all simply different forms of technical information. See 15 C.F.R. pt. 772. In sum, the government's attempt to distinguish source code from other forms of information is unavailing. In essence, the government seeks to justify its pre-publication review of what it concedes to be speech (source code) that has a particular kind of content (encryption algorithms) by declaring that such speech is merely a "product."

The government could not escape First Amendment scrutiny of pre-publication restraints on information or music published on CD-ROM or audiotape simply by labeling these items "products" rather than "information." This instant attempt must fail for the same reasons.

B. Encryption information is not free from the Regulations' licensing restrictions. '

The government attempts to support its pre-publication licensing requirements on encryption software by suggesting that the Export Administration Regulations impose no licensing restrictions on the ability of Professor Bernstein or anyone else to disseminate other kinds of encryption information. See Brief of Appellant at 20, 29. That suggestion cannot withstand scrutiny.

The Regulations plainly make encryption information -- defined as information for the development, production, or use of encryption -- subject to the very same licensing requirements that apply to encryption hardware and encryption software. See 15 C.F.R. " 736.2(b)(1), (2), (3); 738 & Supp. 1, pt. 774, ECCN 5E002. The government points to certain exceptions in the Regulations for information that has become "publicly available" through certain limited and specifically defined means./ But it is undeniable that some encryption information will fall outside these exceptions and will therefore remain subject to the full force of the Regulations' licensing requirements. Indeed, in its discussion of the appropriate remedy in this case, the government not only recognizes that encryption information is subject to full EAR licensing control, but also argues that any remedy must leave those controls in place. See Brief of Appellant at 47-48.

III. The Export Administration Regulations constitute an unconstitutional prior restraint on protected expression.

A. The Regulations represent a classic prior restraint that fails to comport with the Pentagon Papers standard.

Because the Regulations require an individual to secure a government-issued license before the publication or dissemination of protected expression outside the United States/ -- or even inside the United States via the Internet or to foreign nationals -- they embody a classic form of prior restraint on expression. The Supreme Court has repeatedly held that

> [a statute which] makes the peaceful enjoyment of freedoms which the Constitution guarantees contingent upon the uncontrolled will of an official -- as by requiring a permit or license which may be granted or withheld in the discretion of such official -- is an unconstitutional censorship or prior restraint upon the enjoyment of those freedoms.

Shuttlesworth v. Birmingham, 394 U.S. 147, 150-51 (1969). As the Supreme Court explained early in this century, "the chief purpose of the guarantee [of freedom of expression] [is] to prevent previous restraints upon publication," as prior restraints are "the essence of censorship." Near v. Minnesota, 283 U.S. 697, 713 (1931); see also id. at 713-15 (describing our Nation's centuries-old history of repugnance toward prior restraints).

Accordingly, "[a]ny system of prior restraints of expression comes to [the] Court bearing a heavy presumption against its constitutional validity." Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70 (1963); see also New York Times Co. v. United States, 403 U.S. 713, 714 (1971) (per curiam).

In any case involving a prior restraint on protected expression, such as that embodied in the Regulations, the government "carries a heavy burden of showing justification for the imposition of such a restraint." Id. The First Amendment's ban on prior restraints may be overridden only where the government conclusively establishes that the regulation falls within the one recognized exception to the ban on prior restraints applicable in cases involving national security concerns. This exception has been construed very narrowly. It is met only where "[publication] will surely result in direct, immediate, and irreparable damage to our Nation or its people," id. at 730 (Stewart, J., joined by White, J., concurring), or where there is "governmental allegation and proof that publication must inevitably, directly, and immediately cause the occurrence of an event kindred to imperiling the safety of a transport already at sea," id. at 726-27 (Brennan, J., concurring); see also Burch v. Barker, 861 F.2d 1149, 1154 (9th Cir. 1988) ("Prior restraints are permissible only in the rarest of circumstances, such as imminent threat to national security.") (emphasis added).

This narrow exception to the prohibition on prior restraints "refers to the fact that, as a matter of procedural safeguards and burden of proof, prior restraints even within a recognized exception to the rule against prior restraints will be extremely difficult to justify." Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 592 (1976) (Brennan, J., joined by Stewart, J., and Marshall, J., concurring). Even within the sole possible exception to the prohibition against prior restraints, therefore, the government's burden is "formidable," and indeed "almost insuperable." Id. at 593-94. Thus, for example, despite the government's assertion that the publication of a classified Defense Department study would interfere with national security, produce the death of military personnel, and prolong the Vietnam War, the Supreme Court refused to uphold a prior restraint imposed on publication, holding that the government failed to meet its "'heavy burden of showing justification for the imposition of such a [prior] restraint.'" New York Times, 403 U.S. at 714 (per curiam).

In the instant case, the government does not contend that the publication or dissemination of the text at issue will cause "direct, immediate, and irreparable damage to our Nation or its people," id. at 730 (Stewart, J., joined by White, J., concurring), or that there is an "imminent threat to national security," Burch, 861 F.2d at 1154. Nor could it. The Regulations allow the government to prohibit the dissemination of source code with cryptographic content based on nothing more than a determination that the prohibition "is consistent with U.S. national security and foreign policy interests." 15 C.F.R. ' 742.15(b). This sort of discretionary, standardless pre-publication review of protected expression fails to satisfy the standard set forth in New York Times and poses the grave dangers of a censorship system that the Supreme Court and this Circuit have repeatedly condemned. See, e.g., Niemotko v. Maryland, 340 U.S. 268 (1951); Desert Outdoor Advertising v. City of Moreno Valley, 103 F.3d 814, 818 (9th Cir. 1996) ("A law subjecting the exercise of First Amendment freedoms to the prior restraint of a license, without narrow, objective, and definite standards to guide the licensing authority, is unconstitutional.") (internal quotations omitted), cert. denied, 66 U.S.L.W. 3281 (1997).

Because the Regulations embody a classic form of prior restraint on protected expression in which undue discretion is vested in a government licensor, see Shuttlesworth, 394 U.S. 147; Desert Outdoor Advertising, 103 F.3d 814, and that does not comply with the standard of New York Times, the Regulations' licensing scheme is unconstitutional.

B. The prior restraint embodied in the Regulations is also unconstitutional because it fails to provide necessary procedural safeguards.

The Regulations embody a prior restraint that should be found unconstitutional for a second, independent reason: here, as in FW/PBS, the statutory scheme lacks the fundamental procedural safeguards that the Supreme Court has repeatedly identified as essential to a government licensing scheme. See, e.g., Freedman v. Maryland, 380 U.S. 51 (1965); Teitel Film Corp. v. Cusack, 390 U.S. 139 (1968) (per curiam).

To pass constitutional muster, all prior restraints on protected expression -- even content-neutral prior restraints -- must provide at least two procedural safeguards: (1) there must be definite and reasonable limitations on the time within which the licensor must decide whether to issue the license; and (2) expeditious judicial review of the licensing decision must be available. See Freedman, 380 U.S. at 58-59; Bantam Books, 372 U.S. at 70; FW/PBS, 493 U.S. at 227-30. The government suggests that content-neutral prior restraints, or prior restraints that are not directed at preventing the public exchange of information or ideas, need not comport with these procedural safeguards. See Brief of Appellant at 21. But even assuming arguendo that the Regulations were content-neutral, that would not save the Regulations from scrutiny under the prior restraint doctrine. As the Fourth Circuit sitting en banc explained in Baltimore Boulevard,

> [T]he [Supreme] Court has made clear that otherwise valid content-neutral . . . restrictions that require governmental permission prior to engaging in protected speech must be analyzed as prior restraints and are unconstitutional if they do not limit the discretion of the decision-maker and provide for the Freedman procedural safeguards.

11126 Baltimore Boulevard v. Prince George's County, Md., 58 F.3d 988, 995 (4th Cir.) (en banc), cert. denied, 116 S. Ct. 567 (1995). The Supreme Court concluded in FW/PBS that the above procedural safeguards must be provided in any system of prior restraint, regardless of whether it is content-neutral or content-based. Id.; see also Lakewood v. Plain Dealer Publishing, 486 U.S. 750, 764 (1988) ("[E]ven if the government may constitutionally impose content-neutral prohibitions on a particular manner of speech, it may not condition that speech on obtaining a license or permit from a government official in that official's boundless discretion.").

The Regulations in this case are therefore subject to and deficient in light of the above prior restraint analysis, even assuming arguendo that they are content-neutral. Similarly -- and contrary to the government's assertions --

regardless of whether the Regulations were specifically intended or designed to prevent the public exchange of information or ideas, regulations with the effect of restraining expression prior to its publication are subject to the prior restraint doctrine. For example, in Lakewood, despite the government's contention that the regulations on newsracks were designed to protect the health, safety and welfare of citizens -- not to prevent the public exchange of ideas or information -- the regulations were found subject to and deficient under the prior restraint doctrine. See id. at 770.

The Regulations fail to provide the required procedural safeguards for prior restraints, first, because they fail to impose time limits on the government's licensing determinations./ "A prior restraint on speech that imposes no time limitations on the decision-making process plainly fails to satisfy the first requirement set forth in Freedman." Baltimore Boulevard, 58 F.3d at 997; see also FW/PBS, 493 U.S. at 227. Although the reasonableness of the time period of the licensor's decision-making process may vary in different contexts depending on the type of judgments involved in the licensing determination, an open-ended time frame such as that permitted under the Regulations clearly lacks this essential procedural safeguard. See United States v. Thirty-Seven Photographs, 402 U.S. 363, 374 (1971); Baltimore Boulevard, 58 F.3d at 997; see also Teitel Film, 390 U.S. at 141-142 (per curiam) (finding that 50-57 day period for obtaining an administrative decision in film censorship context did not amount to a "specified brief period" for purposes of the Freedman analysis).

Second, the Regulations fail to provide for prompt judicial review of the government's licensing decision. The Supreme Court has repeatedly emphasized the importance of the availability of expeditious judicial review of licensing determinations in the prior restraint context. See Freedman, 380 U.S. at 58-59; Thirty-Seven Photographs, 402 U.S. at 368. In the case of licensing decisions under the Regulations, the executive branch apparently takes the position that judicial review is completely unavailable./ Amici are aware of no case in which a federal court has upheld a regulation imposing a prior restraint on protected expression where judicial review of the licensor's decision was unavailable. See Baltimore Boulevard, 58 F.3d at 1000-01 (collecting cases).

In sum, the Regulations impose a prior restraint on protected expression that does not satisfy the requirements of New York Times and vests undue discretion with the government licensing official. Even assuming arguendo that the Regulations embodied an otherwise valid, content-neutral licensing scheme, the scheme would nonetheless be unconstitutional because it fails to provide definite and reasonable limitations on the time within which the government must issue its licensing determinations and fails to provide for prompt judicial review of licensing determinations. Thus, the Regulations constitute a system of unconstitutional prior restraint of protected expression in violation of the First Amendment.

IV. The Export Administration Regulations constitute an unconstitutional content-based regulation of protected speech.

Even if this Court finds that the Regulations do not impose an unconstitutional prior restraint, the Regulations should be struck down because they embody a content-based restriction on expression that is not narrowly tailored to serve a compelling governmental interest. Under the Regulations, the government seeks to restrict the dissemination of certain text on the basis of its content because the government considers such expression to be inimical to national security and foreign policy interests. If the source code at issue embodied word processing algorithms, for example, instead of encryption algorithms, the Regulations would not restrict its dissemination. The government expressly concedes that the Regulations distinguish encryption software from all other software and impose more onerous restrictions based solely on software's encryption content. See Brief of Appellant at 12-13, 44. Thus, even if not analyzed as a prior restraint, the Regulations' licensing scheme is constitutionally suspect because it is aimed at the suppression of a category of allegedly dangerous expression.

Because the Regulations restrict expression based on its content, they are subject to heightened First Amendment scrutiny. See, e.g., Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37 (1983); Police Dep't of Chicago v. Mosley, 408 U.S. 92 (1972). As the Supreme Court explained in Mosley, a government regulation that delineates permissible and impermissible expression in terms of its content or subject matter is unconstitutional, absent a compelling governmental interest and narrow tailoring of means to end. Id. at 95 ("[A]bove all else, the First Amendment means that government has no power to restrict expression because of its . . . subject matter, or its content."). The government does not contend that the Regulations can withstand such strict scrutiny.

A. The government's proposed analyses for finding the Regulations content-neutral are erroneous. '

The government offers several arguments to support its contention that the Regulations are content-neutral and therefore subject to reduced scrutiny. First, the government contends that regulations cannot be considered content-based unless they are motivated by the government's express disagreement with the message conveyed by the regulated expression. See Brief of Appellant at 25. Second, the government argues that regulations premised upon national security or foreign policy concerns should not be considered content-based. Id. at 25-26. Third, the government contends that the Regulations are content-neutral because they restrict both expression and non-expression (i.e., both cryptographic software and hardware). Id. at 42. The flaws in each of these contentions are apparent.

First, the government errs in contending that whether a regulation is content-neutral turns on whether it was motivated by an illicit governmental intent. The Supreme Court has rejected the notion that First Amendment analysis requires courts to peer into the subjective minds of the legislators who enact the restrictions at issue. As the Court explained in Minneapolis Star & Tribune Co. v. Minnesota Comm'r of Revenue:

> Illicit legislative intent is not the sine qua non of a violation of the First Amendment. We have long recognized that even regulations aimed at proper governmental concerns can restrict unduly the exercise of rights protected by the First Amendment.

460 U.S. 575, 592 (1983) (citations omitted). Second, throughout this

century the Supreme Court has recognized that government censorship motivated by concerns for national security or foreign policy can still constitute invalid content-based regulations. See, e.g., New York Times Co. v. United States, 403 U.S. 713 (1971); see also Bullfrog Films, Inc. v. Wick, 847 F.2d 502 (9th Cir. 1988)./ There is no per se exception to the First Amendment for speech that concerns national security or foreign policy. Third, the government's argument that it can constitutionally restrict expression because it also restricts non-expression cannot save the Regulations from constitutional attack. Accepting this novel First Amendment rationale would mean, for example, that localities could restrict a host of items considered to be dangerous -- for example, guns and knives and "dangerous" books -- and could then contend that these regulations were content-neutral simply because non-expressive as well as expressive items were regulated. It is surely no answer to a complaint of a First Amendment violation that the subject regulations concededly restrict expressive activity, but also prohibit other, non-expressive activity.

B. The functionality or usefulness of the text at issue does not withdraw it from First Amendment protection.

The government correctly notes that Lakewood v. Plain Dealer provides for stringent First Amendment scrutiny of regulations burdening items or activities that are "commonly associated with expression." The government contends, however, that the source code at issue is not commonly associated with expression because of what the government contends are its unique functional qualities. It contends that encryption software is regulated, whereas books containing source code are not, because of the unique functional qualities of software. This argument is also without merit.

Although it is certainly true that it is easier to encrypt communications if one has encryption source code stored on disk rather than printed in a book, this difference is one of degree and bears no constitutional significance. To convert source code printed in a book to a computer readable format, the user must have some minimal additional knowledge (how to type or scan the text into the computer) and must press more keys on a computer to accomplish the task. Once these steps are taken, the source code printed in the book can be used to encrypt communications. But the usefulness or "functionality" of speech is always a product of the existing knowledge and facility of the reader. Thus, a person sent a copy of the Pythagorean Theorem who understands the meaning of the word "hypotenuse" and who has a calculator will find the theorem quite functional, compared to a person without such tools or skills. Similarly, exportation of Mao's Little Red Book in Chinese is less "functional" as an instructional text to people in Latin America than is the identical book translated into Spanish. In neither case would variations in the "functionality" of the speech justify its suppression in one case but not the other. Similarly, in the instant case, the functionality of the text at issue stored on disk cannot justify its suppression./

C. Even if the Regulations were not subject to strict scrutiny, they are unconstitutional because they are not narrowly tailored.

For the reasons set forth above, the government's argument that the Regulations are content-neutral should fail. Even if, however, one were to accept the government's position that the First Amendment requires only that the Regulations must further an important government interest, be unrelated to the suppression of free expression, and be narrowly tailored, the Regulations would still be unconstitutional. Amici agree that national security is an important governmental interest. Even accepting the government's argument, however, the Regulations cannot be considered narrowly tailored.

The government concedes that speech comparable to or even virtually identical to the speech regulated in this case is available overseas. See Brief of Appellant at 33. The government also concedes that the exact speech in this case can be exported in book form. Given these concessions, it is difficult to see the Regulations as narrowly tailored to the purpose of preventing those overseas from encrypting messages. Even if the Regulations were fully enforced, those overseas and hostile to the United States could encrypt their messages by using comparable software available overseas, by downloading nearly identical software from one of many Internet sites, or by converting the printed source code into electronic form. Speech-restrictive regulations that fail to accomplish their stated purpose to any significant degree cannot be found "narrowly tailored" and must be held unconstitutional even under intermediate constitutional scrutiny.

V. The Regulations unreasonably and impermissibly burden private speech.

The source code at issue in this case not only constitutes expression that merits First Amendment protection, as discussed above, but is also critical to safeguard the right of private speech, which implicates important First and Fourth Amendment values. Regulations on cryptographic software such as those embodied in the Regulations have the effect of controlling the result -- private speech -- by controlling the tools necessary to achieve that result in the electronic sphere. As the Supreme Court has long held, the government may not target the tools of expression to restrain or burden the underlying expression itself. See, e.g., Minneapolis Star, 460 U.S. at 585. As discussed below, regulations on cryptographic software chill private electronic communications, impermissibly burden constitutionally protected speech, and interfere with people's reasonable expectation of privacy in their electronic communications.

A. Communications via the Internet, especially private communications, are an increasingly important form of expression.

The Internet has quickly become an unprecedented forum for communication among individuals throughout the United States and indeed the entire world. As the special 3-judge panel in ACLU v. Reno explained,

> It is no exaggeration to conclude that the Internet has achieved, and continues to achieve, the most participatory marketplace of mass speech that this country -- and indeed the world -- has yet seen. [Because of the special characteristics of Internet communications,] the Internet deserves the broadest possible protection from government-imposed . . . regulation.

ACLU v. Reno, 929 F. Supp. 824, 881 (E.D.Pa. 1996), aff'd, 117 S. Ct. 2329 (1997). The court explained further that "[t]he World Wide Web exists fundamentally as a platform through which people and organizations can communicate through shared information." Id. at 837. Each day, millions of items of text, messages, and other communications are exchanged among the participants on the Internet, which serves as an unrivaled forum for free expression and the exchange of ideas.

B. Private communications, including private electronic communications, are protected by the convergence of First and Fourth Amendment values.

Encryption capabilities are essential to the ability to communicate privately in the information age. Without readily-available encryption software, confidential or private electronic communications are rendered vulnerable to public exposure and interception. To require electronic communications and records to be unencrypted is equivalent to requiring that all paper communications be written on postcards instead of conveyed in sealed envelopes. Regulations that impose a significant burden on the dissemination of encryption software have a similar effect. If effective encryption is difficult to obtain, the result will be that private messages and records will be vulnerable to unwilling disclosure. That result is inconsistent with the mandate of the ACLU v. Reno court that "the Internet deserves the broadest possible protection" from government regulation. Id. at 881.

Courts have also long recognized that the Fourth Amendment shields private communications from unreasonable governmental interference or surveillance. See, e.g., United States v. United States District Court, 407 U.S. 297 (1972) ("Keith"); Katz v. United States, 389 U.S. 347 (1967). In particular, the Supreme Court has held that "governmental incursions into conversational privacy" via electronic means "necessitate the application of Fourth Amendment safeguards." Keith, 407 U.S. at 313. Throughout this century, the importance of communications privacy has been recognized, regardless of whether the medium of private communication is a sealed letter or a telephonic or electronic message. See Olmstead v. United States, 277 U.S. 438, 472-75 (1928) (Brandeis, J., dissenting) (fearing government's eventual use of "subtler and more far-reaching means of invading privacy [furnished through] the progress of science."). The Supreme Court has explained that when the government seeks to impinge upon private communications in the name of national security, the "convergence of First and Fourth Amendment values" must guide the Court's interpretation of the reasonableness of the government's interference. Keith, 407 U.S. at 313.

The Internet has become an increasingly important forum for private communications. Individuals throughout the United States have come to expect that their electronic communications, and often their identities, will be shielded from public view. See, e.g., ACLU v. Reno, 929 F. Supp. at 849 (recognizing importance of preserving privacy of identity of participants in Internet communications); Shea v. Reno, 930 F. Supp. 916, 941 (S.D.N.Y. 1996) (same); ACLU v. Miller, 43 U.S.P.Q.2d (BNA) (N.D. Ga. 1997) (finding substantial likelihood that statute compelling identity of Internet communicant was unconstitutional). Courts have explicitly recognized that those who send private electronic communications enjoy a reasonable expectation of privacy in the content of those communications, such that government officials may not access such communications without probable cause and a search warrant. See, e.g., United States v. Maxwell, 45 M.J. 406

(C.A.A.F. 1996).

Without readily-available encryption software, however, electronic communications can be easily intercepted, and communications intended to be private may be rendered vulnerable to exposure. As the district court in ACLU v. Reno recognized, electronic messages sent over the Internet are not "`sealed' or secure, and can be accessed or viewed on intermediate computers between the sender and the recipient (unless the message is encrypted)." 929 F. Supp. at 834 (emphasis added). Similarly, the district court in American Library Association v. Pataki lamented the insecurity of electronic communications via the Internet relative to communications via U.S. mail, noting that "[w]hile first class letters are sealed, e-mail communications are more easily intercepted." American Library Association v. Pataki, 969 F. Supp. 160, 165 (S.D.N.Y. 1997). That court went on to note that "[c]oncerns about the relatively easy accessibility of e-mail communications have led bar associations in some states to require that lawyers encrypt sensitive e-mail messages in order to protect client confidentiality." Id.

Cryptography has also become an increasingly vital tool for political dissidents, human rights activists, and whistle-blowers in the United States and throughout the world to facilitate private electronic communications free from intrusion. See, e.g., David Banisar, A Primer on Electronic Surveillance for Human Rights Organizations, International Privacy Bulletin 3 (July 1993); Zimmermann Decl. & 25 (ER 00196) (human rights organizations rely upon the unfettered use of cryptography to protect their communications, as do witnesses who report human rights abuses in repressive regimes throughout the world).

The Regulations' restrictions on the dissemination of cryptographic software, however, render it difficult for those communicating via the Internet or other electronic means to achieve genuine privacy. The Regulations substantially constrain private communications between people in the United States and people located in other countries -- whether U.S. citizens or foreign nationals. This is a result of the critical importance of "interoperable" software to the global Internet: Unless both parties to the communication share encryption software that employs the same cryptographic methods and standards, they cannot communicate privately at all. The Regulations, and the restrictive licensing policies they embody, effectively prevent most U.S. persons from communicating privately with those in foreign countries.

The Regulations also have an indirect impact on the development and availability of effective encryption software even within the United States. If a strong and effective encryption system can be sold only in the United States, or sold elsewhere only after a lengthy and burdensome process of obtaining licensing approval for every individual sale, its marketability is diminished. Producers will not only forfeit world-wide sales altogether, but even U.S. customers who want to communicate globally may not find such products attractive. The result is that certain software producers have declined to develop strong encryption features in mass-market products, particularly word processing and spreadsheet software, which integrate cryptographic capabilities. Some U.S. software developers have elected to produce only software with relatively ineffective encryption features that are not subject to the Regulations' restrictions and can readily be sold abroad. As the report of the National Research Council's Committee to Study Cryptography concluded, "U.S. export controls have had a negative impact on the cryptographic strength of many integrated products with encryption capabilities available in the United States." NRC Report, supra, ' 4.3.1 (footnote omitted).

In sum, the Export Administration Regulations' pre-publication restrictions on encryption software impermissibly and unreasonably burden the development, availability, and use of encryption, which is the sine qua non of private electronic communications. Regulations that burden rights protected by the First Amendment are unconstitutional, absent a compelling government interest. See Minneapolis Star, 460 U.S. at 585. As no such compelling government interest exists in this case, the Regulations should be struck down.

CONCLUSION

For the reasons stated above, the judgment of the District Court below should be affirmed.

Respectfully submitted,

Ivan K. Fong
Dawn C. Nunziato
David W. Addis
COVINGTON & BURLING
1201 Pennsylvania Ave., N.W.
P.O. Box 7566
Washington, DC 20044
(202) 662-6000

David L. Sobel
Marc Rotenberg
ELECTRONIC PRIVACY
INFORMATION CENTER
666 Pennsylvania Ave., SE
Washington, DC 20003
(202) 544-9240

Counsel for Amici Curiae

Date: November 7, 1997

FOOTNOTES

1 / The State Department belatedly notified Bernstein, after this suit commenced, that the Snuffle source code was an ITAR-controlled "defense article," that the related Snuffle instructions were ITAR-controlled "technical data," but that the Snuffle scientific paper was not subject to the ITAR. See Bernstein Decl. & 41 (ER 00013).

2/ The Regulations were originally promulgated by authority of the Export Administration Act ("EAA" or "Act"), 50 U.S.C. App. " 2401-2420. The EAA has lapsed and has not been reenacted by Congress. The provisions of both the EAA and EAR are kept in force by executive orders exercising the President's emergency powers under the International Emergency Economic Powers Act ("IEEPA"), see 50 U.S.C. " 1701-1706; 62 Fed. Reg. 43,629 (August 15, 1997); 59 Fed. Reg. 43,437 (August 23, 1994).

3 / The exceptions from these expansive licensing requirements are limited to certain forms of "publicly available" technology that are embodied in books, periodicals, or recordings; generally available at libraries or open conferences; submitted to professional journals; part of academic instruction; or that result from certain fundamental research. These exceptions, however, do not extend to encryption source code in any electronic form, which remains fully subject to the Regulations licensing requirements. See 15 C.F.R. ' 734.3(b)(2), (3). Thus, while encryption source code can be freely published and disseminated in book form, the identical source code in electronic form is subject to pre-publication licensing.

4 / The economic significance of cryptographic technology has been recognized internationally. In a policy declaration entitled "Towards a European Frame work for Digital Signatures and Encryption," the European Commission recently observed that "In order to make good use of the commercial opportunities offered by electronic communication via open networks, a secure and trustwor thy environment is . . . necessary," (visited October 23, 1997) <http://www.ispo .cec.be/eif/ policy/97503.html> (hereinafter "European Encryption Declaration") (attached at Appendix A). Likewise, the Organization for Economic Coopera tion and Development ("OECD") has recognized that

[T]he failure to utilise cryptographic methods can adversely affect the protection of privacy, intellectual property, business and financial information, public safety and national security and the operation of electronic commerce because data and communications may be inadequately protect ed from unauthorized access, alteration, and improper use, and, therefore, users may not trust information and communications systems, networks and infrastructures.

OECD Cryptography Policy Guidelines (March 27, 1997) <http://www.oecd.org /dsti/iccp/crypto_e.html> (attached at Appendix A).

5 / As reported in the "European Encryption Declaration," supra note 4, encryp tion technology firms are now migrating overseas, with 440 non-U.S. firms compared to 400 U.S. firms.

6 / See Paul Swamidass, Technology on the Factory Floor III (forthcoming 1998).

7 / See Statement of Louis J. Freeh, Director, Federal Bureau of Investigation, before the Senate Select Committee on Intelligence and the Senate Judiciary Committee on Terrorism, Technology and Government Information, February 28, 1996.

8 / A segment of the actual source code at issue in this case is set forth below:

```
SetupHash512();

for (i = 0; i < 64;i++)

x[i] = k[i] = h[i] = 0;

 /* What matters is x[9...63], y, k[0...63], h[0...63]. */

if (!fi)

exit(2);
```

9 / Copyright law also supports, by analogy, the extension of the First Amend ment to encompass source code. The copyright statute contemplates that scientists will use computer programs as a vehicle for expressing their ideas, and the protection of copyright law extends to the expression of ideas embodied in computer programs. See H.R. Rep. No. 94-1476 at 54 (1976), reprinted in 1976 U.S.C.C.A.N. 5659, 5667; Final Report of the National Commission on New Technological Uses of Copyrighted Works ("CONTU") (1976); see also 17 U.S.C. ' 101, at 878 (1994) (granting copyright protection to works "expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as books, . . . tapes, disks, or cards, in which they are embodied"); 17 U.S.C. ' 102(a)(1) (1994); Berne Convention for the Protection of Literary and Artistic Works, Art. 2 (extending copyright protection to computer programs as literary works); World Intellectual Property Organization Copyright Treaty, Art. 4 (1996) (same); Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240, 1249 (3d Cir. 1983) (extending copyright protection to source code as a "literary work"), cert. dismissed, 464 U.S. 1033 (1984). Furthermore, the Supreme Court has explained that the Copyright Act's protection of the expression of ideas embodies the core values of the First Amendment. See Harper & Row Publishers, Inc. v. Nation Enter., 471 U.S. 539 (1985).

10/ The Regulations define specific "publicly-available" criteria for information embodied in books, periodicals, or recordings; generally available at libraries or open conferences; submitted to professional journals; result from certain funda mental research; or part of academic instruction. 15 C.F.R. " 734.3(b)(2), (3), 734.7, 734.8, 734.9.

11 / The purview of the First Amendment protec tion of expression does not apply solely to communications among U.S. citizens, nor does it stop at the Nation's borders. See Bullfrog Films, Inc. v. Wick, 847 F.2d 502 (9th Cir. 1988).

12 / Although the Regulations provide that "license applications will be resolved or referred to the President" within 90 days, that time limit may be tolled by a variety of circumstances or government actions. See 15 C.F.R. ' 750.4(a)(1). The regulations also contemplate a cumbersome and lengthy inter-agency review process. If the license application is denied at an initial stage, the denial may then be appealed to other officials within the

Commerce Department, and the appeal procedures impose no deadline other than "a reasonable time" for a final decision. 15 C.F.R. ' 756.2(c)(2). Likewise, if the matter is referred to the President, as the Regulations allow, no deadline is prescribed for the President's decision.

13 / The Export Administration Act expressly precludes judicial review. See 50 U.S.C. App. ' 2412(e). Reflecting that rule, the Regulations flatly declare that "the decision of the Under Secretary shall be final." 15 C.F.R. ' 756.2(c). The Act and the Regulations are both kept in force by an exercise of the President's authority under the International Emergency Economic Powers Act, which has no similar provision expressly precluding judicial review. However, the Presi dent's executive order provides that "[t]o the extent permitted by law," all of the provisions of the Act and the Regulations -- presumably including the bar to judicial review -- shall "continue in full force." E.O. 12924, 59 Fed. Reg. 43,437 (Aug. 23, 1994).

14 / International law binding upon the United States also requires careful scrutiny of restrictions on speech justified in the name of national security. See, e.g., International Covenant on Civil and Political Rights, 999 U.N.T.S. 171 (ratified by U.S. 1992) (permitting restriction of the right to freedom of expression in the interest of national security only where "necessary.").

15 / It is not harmless to suppress the speech in disk form while allowing it in print form. The Supreme Court has repeatedly held that the fact that one forum exists for speech does not mean that such speech can be suppressed in other fora. See Reno v. ACLU, 117 S. Ct. 2329 (1997).

16 / The private speech interests facilitated by cryptography are recognized internationally, as well as in the United States. Fifteen international human rights and civil liberties organizations, including amici EPIC, ACLU, CPSR, HRW, and PI, recently endorsed a "Resolution in Support of the Freedom to Use Cryptography." The resolution notes that "the use of cryptography impli cates human rights and matters of personal liberty that affect individuals around the world," and that "the privacy of communication is explicitly protected by Article 12 of the Universal Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights, and national law." See Resolution in Support of the Freedom to Use Cryptography, (Sept. 25, 1996) <http://www.gilc.org/gilc/ resolution.html> (attached at Appendix A).

17/ By impinging upon individuals' efforts to communicate privately, the Regulations also run afoul of the International Covenant on Civil and Political Rights, which specifically protects the rights of individuals worldwide "to receive and impart information and ideas of all kinds, regardless of frontiers," through "writing," "print," or "any other media of [their] choice."

CERTIFICATE OF COMPLIANCE

I hereby certify that this Brief of Amici Curiae has side margins of 1 inch, top and bottom margins of 1-1/4 inch, and double spaced text, except as otherwise permitted under Circuit Rule 32. I further certify that the word processor used to prepare this brief reports that this brief is printed in 14 point Times Roman font, a proportionately spaced typeface, and that the relevant portions of this brief contain 13,334 words.

Dawn C. Nunziato
COVINGTON & BURLING
1201 Pennsylvania Ave., N.W.
P.O. Box 7566
Washington, DC 20044

Counsel for Amici Curiae

RELATED CASES

Amici do not know of any related cases pending in this Court.

CERTIFICATE OF SERVICE

I hereby certify that I have, this 7th day of November, 1997, arranged to send by overnight courier two copies of the foregoing Brief of Amici Curiae to:

Douglas N. Letter
Scott R. McIntosh
Attorneys, Appellate Staff
Civil Division, Room 9550
Department of Justice
601 D Street, N.W.
Washington, DC 20530-0001

Robert Corn-Revere
Hogan & Hartson, L.L.P.
555 Thirteenth Street, NW
Washington, DC 20004

Cindy A. Cohn
McGlashan & Sarrail
177 Bovet Road, Sixth Floor
San Mateo, CA 94402

Dawn C. Nunziato
COVINGTON & BURLING
1201 Pennsylvania Ave., N.W.
P.O. Box 7566
Washington, DC 20044

Counsel for Amici Curiae