C.A. 98-4045

IN THE
UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

PETER JUNGER
Plaintiff/Appellant,
v.
WILLIAM M. DALEY, UNITED STATES SECRETARY OF COMMERCE, ET AL.,
Defendants/Appellee

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

BRIEF FOR *AMICI CURIAE*

ELECTRONIC PRIVACY INFORMATION CENTER; ASSOCIATION OF INFORMATION TECHNOLOGY PROFESSIONALS; CENTER FOR DEMOCRACY AND TECHNOLOGY; COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY; EAGLE FORUM; ELECTRONIC FRONTIER FOUNDATION; FREE CONGRESS RESEARCH AND EDUCATION FOUNDATION; HUMAN RIGHTS WATCH; INTERNATIONAL INFORMATION SYSTEM SECURITY CERTIFICATION CONSORTIUM; INTERNET SOCIETY; NATIONAL ASSOCIATION OF MANUFACTURERS; PRIVACY INTERNATIONAL; U.S. PUBLIC POLICY COMMITTEE OF THE ASSOCIATION FOR COMPUTING; DR. WHITFIELD DIFFIE; DR. PETER NEUMANN; DR. RONALD RIVEST; and MR. BRUCE SCHNEIER

IN SUPPORT OF APPELLANT PETER JUNGER AND REVERSAL OF THE JUDGMENT BELOW

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

Kurt A. Wimmer
David W. Addis
COVINGTON & BURLING
1201 Pennsylvania Ave., N.W.
P.O. Box 7566
Washington, DC 20044-7566
(202) 662-6000

Counsel for *Amici Curiae*

March 8, 1999

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

C.A. 98-4045

PETER JUNGER
Plaintiff/Appellant,
v.
WILLIAM M. DALEY, UNITED STATES SECRETARY OF COMMERCE, ET AL.,
Defendants/Appellee.

DISCLOSURE OF CORPORATE AFFILIATIONS AND FINANCIAL INTEREST

Pursuant to Sixth Circuit Rule 26.1, *Amici Curiae* Electronic Privacy Information Center; Association of Information Technology Professionals; Center for Democracy and Technology; Computer Professionals for Social Responsibility; Eagle Forum; Electronic Frontier Foundation; Free Congress Research and Education Foundation; Human Rights Watch; International Information System Security Certification Consortium; Internet Society; National Association of Manufacturers; Privacy International; and U.S. Public Policy Committee of the Association for Computing make the following disclosures:

1. Are said parties subsidiaries or affiliates of a publicly owned corporation? NO.

If the answer is YES, list below the identity of the parent corporation or affiliate and the relationship between it and the named party. NOT APPLICABLE.

2. Is there a publicly owned corporation, not a party to the appeal, that has a financial interest in the outcome? NO.

March 8, 1999

David W. Addis
Attorney for *Amici Curiae*

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

FEDERAL STATUTES AND REGULATIONS

OTHER SOURCES

INTERESTS OF *AMICI CURIAE*

All parties have consented to filing this brief.

The Electronic Privacy Information Center ("EPIC") is a non-profit, public interest organization focusing on civil liberties issues in the field of electronic information, with both legal and technical expertise in encryption.

The Association of Information Technology Professionals is a non-profit organization providing leadership and education in information technology.

The Center for Democracy and Technology is a non-profit, public interest organization dedicated to advancing individual liberty in new digital communications media.

Computer Professionals for Social Responsibility is an alliance of computer scientists and others concerned about the impact of computer technology on society.

The Eagle Forum is a conservative, pro-family and pro-life grassroots organization dedicated to preserving personal liberty.

The Electronic Frontier Foundation is a non-profit organization working to ensure that the principles of the Bill of Rights are protected as new communications technologies emerge.

The Free Congress Research and Education Foundation is a non-profit foundation dedicated to conservative governance, and concerned about protecting personal privacy in the face of advancing technologies.

Human Rights Watch is a non-profit organization that investigates and reports violations of human rights worldwide, and uses encryption as a means to protect human rights advocates from government reprisals.

The International Information System Security Certification Consortium is a non-profit organization of information system security professionals that promotes prudent information security measures.

The Internet Society is an international organization for worldwide coordination of Internet issues. It serves to assure the open evolution of the global Internet and internetworking technologies.

The National Association of Manufacturers is the nation's oldest and largest broad-based industrial trade association. Its more than 14,000 members employ approximately 85 percent of all manufacturing workers and produce over 80 percent of the nation's manufactured goods.

Privacy International is an international human rights group that monitors surveillance by governments and corporations, and promotes the use of laws and technology to improve personal privacy.

The U.S. Public Policy Committee of the Association for Computing addresses U.S. public policy related to information technology for the Association, a non-profit international scientific and educational organization.

Dr. Whitfield Diffie is Distinguished Engineer at Sun Microsystems, and co-founder of the International Association for Cryptologic Research. He is recognized for his 1975 discovery of the concept of public key cryptography.

Dr. Peter Neumann is Principal Scientist in the Computer Science Laboratory at SRI International and served on the ACM and National Research Council cryptography studies and on the NRC Computers at Risk study.

Dr. Ronald Rivest is the Webster Professor of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology, and a leader of MIT's Cryptography and Information Security research group. Dr. Rivest is an inventor of the RSA Public Key Cryptosystem, and a founder and director of RSA Data Security.

Bruce Schneier is the President of Counterpane Systems, a cryptography and computer consulting firm. He is also the author of *Applied Cryptography*, and a frequent writer and lecturer on cryptography.

STATEMENT OF THE CASE

This case is a First Amendment challenge to the Export Administration Regulations, 15 C.F.R. Parts 730-74 (the "EAR" or the "Regulations"), which restrict the publication and dissemination of encryption software and related technical information.

I. Cryptography

Computers store and exchange an ever-increasing amount of highly personal information, including medical and financial data. Communication and information stored and transmitted by computers can be protected against interception through the use of cryptographic security techniques. *See*, *e.g.*, David Chaum, *Achieving Electronic Privacy*, Scientific American, Aug. 1992, at 96.

Cryptography accomplishes 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, or "key." Only the intended recipient of the

communication, who holds the key, can decrypt and access the information. The key is a string of numbers; the longer the string, the stronger the security. *See*, *e.g.*, Philip R. Zimmerman, *Cryptography for the Internet*, Scientific American, Oct. 1998, at 110.

The authentication capabilities of cryptographic systems involve the use of "digital signatures." A digital signature provides a means of authenticating the integrity of electronically transmitted data and the identity of the sender. *See generally* ABA Science & Technology Section, *Digital Signature Guidelines* (1996).

II. The Export Administration Regulations on Encryption

The Export Administration Regulations impose strict controls for encryption: To export controlled encryption software and technology anywhere except Canada, the exporter must first obtain a license from the Commerce Department. *See* 15 C.F.R. §§736.2(b), 742.15(a).

"Export" is defined expansively to include not only "actual shipment or transmission . . . out of the United States" or "release . . . in a foreign country" — the conventional meaning of "export" — but also certain transfers or disclosures entirely *within* the United States. *See* 15 C.F.R. §§734.2(b)(2), (3), (9).

For encryption software, including source code, "export" includes making the software available on Internet sites or any other "communications facilities" that are merely *accessible* to persons outside the United States, unless certain onerous precautions are taken. 15 C.F.R. §734.2(b)(9)(ii). As the District Court below found, these precautions are "nearly impossible for most Internet users to carry out or verify," so that "almost any posting of software on the Internet is an export." *Junger v. Daley*, 8 F. Supp. 2d 708, 713 (N.D. Ohio 1998).

The result is that (with narrow exceptions not relevant here) a pre-publication license from the Commerce Department is required before publishing or distributing encryption source code or technical information (1) to any person outside the United States and Canada, (2) to any foreign national within the United States, or (3) *to any person at all, inside or outside the United States, by means of the Internet*.

ARGUMENT

I. Text Written in a "High-Level" Programming Language Is Expression Protected Under the First Amendment.

To communicate ideas and information about cryptography, and to encourage discussion and debate, Professor Junger sought and was refused a government determination that text written in C, Perl and other high-level

programming languages could be freely disseminated over the Internet. *See* 8 F. Supp. 2d at 714. The District Court correctly found that software source code is written in a "high-level language" that "can be understood by computer scientists, mathematicians, programmers and others with knowledge of the particular language," and that "people such as Professor Junger can reveal source code to exchange information and ideas about cryptography." *Id.* at 712 n.3, 717. For those very reasons, other courts have recognized that software source code is protected by the First Amendment. *Bernstein v. Dep't of State*, 922 F. Supp. 1426, 1435-36 (N.D. Cal. 1996) ("*Bernstein I*"); 945 F. Supp. 1279 (N.D. Cal. 1996) ("*Bernstein II*"); 974 F. Supp. 1288 (N.D. Cal. 1997) ("*Bernstein III*") (appeal pending); *see also Karn v. Dep't of State*, 925 F. Supp. 1, 9-10 (D.D.C. 1996), *remanded on other grounds*, 107 F.3d 923 (D.C. Cir. 1997). The District Court nevertheless ignored settled First Amendment jurisprudence to hold erroneously that the source code texts at issue here are not entitled to First Amendment protection.

A. The First Amendment protects scientific expression, including text expressed in computer programming languages.

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 in which it is undertaken, it contains sufficient communicative elements. *See Spence v. Washington*, 418 U.S. 405 (1974). Even conduct that is not ordinarily or inherently expressive may be protected under the First Amendment when it is intended to convey a message and is likely to be understood. *Id.* at 409-11. Source code text, however, is more than mere conduct — it is a written high-level language that is inherently expressive.

The District Court correctly found that source code embodies a "high-level language . . . understood by computer scientists, mathematicians, programmers and others with knowledge of the particular language." Trained readers can use this language "to exchange information and ideas about cryptography." 8 F. Supp. 2d at 717; *see also Bernstein I*, 922 F. Supp. at 1435. That determination should end any dispute about whether encryption source code is expression entitled to First Amendment protection. But despite its own unequivocal findings, the District Court dismissed the communicative nature of source code, and refused to give it full protection under the First Amendment, simply because the "broad majority of persons" cannot read or write in source code. 8 F. Supp. 2d at 716-17.

To be granted First Amendment protection, however, expression need not communicate to all members of a community or be meaningful to a general audience. Protected expression may serve as a vehicle for communication among a specialized community, or be meaningful only to certain subsets of society, and includes scientific and artistic speech that might bewilder a reader with no background in the field. Thus the First Amendment's sphere of protection encompasses, for example, abstract paintings, esoteric classical music, rock music, modern dance, and the "Jabberwocky verse of Lewis Carroll." *Hurley v. Irish-American Gay, Lesbian and Bisexual Group*, 515 U.S. 557, 569 (1995); *see also Ward v. Rock Against Racism*, 491 U.S. 781 (1989). Moreover, "it is . . . settled . . . that the First Amendment protects scientific expression and debate just as it protects political and artistic expression." *Stanford Univ. v. Sullivan*, 773 F. Supp. 472, 474 (D.D.C. 1991).

The expression at issue here — source code written in high-level programming languages — is a commonly used and fundamental medium of expression among scientists, mathematicians, programmers and others, as the District Court found. *See* 8 F. Supp. 2d at 712 n.3, 717. Moreover, programming language is a formal vehicle uniquely suited for the precise communication of

complex scientific ideas. As computer scientist Carl Ellison explains, computer languages "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; *see also* Abelson Decl. ¶ 8. It accordingly is clear not only that programming language is expressive, but also that, in many instances, such language is the *only* appropriate vehicle for the communication of precise, complex ideas among scientists, programmers and other computer-literate people.

Thus, the source code at issue is text written in a "high-level" language, *i.e.*, a form of language syntactically and semantically similar to more familiar languages like English or Spanish. *See Encyclopedia of Computer Science* 962, 1263-64 (Ralston & Reilly eds. 3d ed. 1995). 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.[1]

---

[1] The District Court cites two narrowly circumscribed categories of language that are afforded little or no protection under the First Amendment: "fighting words" and false commercial speech. 8 F. Supp. 2d at 716-17. Unlike fighting words or false commercial speech, however, Professor Junger's source code is not

The source code at issue here 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, is protected by the First Amendment.

B. The functional qualities of the text do not diminish its status as protected speech.

Having found, as the District Court did, that source code text is used for communication, it was error to hold that it is without First Amendment protections merely because it is also "inherently functional." The expressive nature of source code text found by the court is equally inherent, and is not altered or diminished by whatever functional qualities it may have. Many kinds of protected speech are inherently and primarily functional. *See Bernstein I*, 922 F. Supp. at 1435. Chemical or mathematical formulae, music scores, and schematic drawings are all inherently functional in the same manner as source code text; each is published and used primarily for its functional value, but each also can be read by trained people, and shared to exchange ideas about chemistry, mathematics,

---

"so removed from any 'exposition of ideas,' and from 'truth, science, morality, and arts in general'" that it should be denied all protection. *Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, 425 U.S. 748, 762 (1976).

music, or engineering. They are all without doubt within the ambit of the First Amendment.

The fact that encryption source code can be transformed into object code, which in turn can provide instructions to a computer, does not distinguish it from these other forms of functional, but protected, speech. The District Court suggests that encryption source code is a "device," like an embedded circuit. 8 F. Supp. 2d at 717. But that simply ignores the court's own findings that source code text, like other functional texts — but unlike an embedded circuit — can be read by trained readers and used to communicate ideas. Moreover, the very Regulations at issue here recognize a fundamental distinction between devices on the one hand, and technical information, including software, on the other. *See* 50 U.S.C. app. §2415(3), (4) (1994); 15 C.F.R. §772.

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 are useless without the aid of a device. *See Freedman v. Maryland*, 380 U.S. 51 (1965); *Reno v. ACLU*, 521 U.S. 844, 117 S. Ct. 2329 (1997). 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 "devices" rather than "information." 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 is read by people and is a preferred vehicle for communication among scientists, programmers, and others.

C. Even if publishing source code could properly be categorized as no more than "conduct with expressive elements," it would still be entitled to First Amendment protection.

For the reasons stated, the District Court erred by concluding that publishing source code text on the Internet, or disseminating it abroad by other means, is no more than "conduct that can occasionally have communicative elements." 8 F. Supp. 2d at 717. Even assuming *arguendo* that the court's determination was correct, however, those activities are still protected by the First Amendment.

The District Court correctly noted that, even for such "occasionally" expressive conduct, First Amendment protections apply where there is "an intent to convey a particularized message" that is likely, "in the surrounding circumstances," to "be understood by those who viewed it." *Id.* (*quoting Spence v.*

State of Washington, 418 U.S. at 411). The court's own findings make clear that publishing or disseminating source code text satisfies the *Spence* guidelines in every respect. There is no dispute that trained people can and do read and write source code, and use it to convey information about cryptography. *See* 8 F. Supp. 2d at 712 n.3, 717. In those circumstances, the message is readily understood by its intended audience. It need not be equally apparent to everyone to merit First Amendment protection. There can be no doubt that many more people in the United States read, write and understand C programming language than read or understand the Finnish or Navajo languages. Symphonic scores and mathematical formulae are similarly addressed to and readily understood by trained readers, while remaining opaque to most laypeople. The act of publishing or disseminating such writings over the Internet is conduct just as clearly within the scope of the First Amendment as publication by any other means. *Reno v. ACLU*, 117 S. Ct. at 2344. The act of publishing or disseminating source code text is similarly protected.

II. The Regulations Constitute an Unconstitutional Prior Restraint on Protected Expression.

A. The Regulations impose prior restraints that fail to comport with First Amendment standards.

The Regulations require a government-issued license before the publication or dissemination of protected expression to anyone — inside or outside the United States — via the Internet. That is a classic prior restraint. 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). The First Amendment's "chief purpose" is "to prevent previous restraints upon publication," the "essence of censorship." *Near v. Minnesota*, 283 U.S. 697, 713 (1931). 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).

1. The government has not and cannot meet its heavy burden to justify the Regulations' prior restraint.

The First Amendment's ban on prior restraints may be overridden only where "[publication] will surely result in direct, immediate, and irreparable damage to our nation or its people," *New York Times*, 403 U.S. 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 WXYZ, Inc. v. Hand*, 658 F.2d 420, 426 (6th Cir. 1981). The government's burden is "formidable," and indeed "almost insuperable." *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 592-94 (1976) (Brennan, J., joined by Stewart, J., and Marshall, J., concurring).

The government does not contend, and the District Court did not find, that the publication or dissemination of the text at issue will result in such imminent and certain harm. No such finding is possible. 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 licensing 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); *Glasson v. City of Louisville*, 518 F.2d 899, 905 (6th Cir. 1975).

2. The Regulations impose a prior restraint directed only at text with cryptographic content.

The District Court reasoned that the Regulations do not impinge upon protected expression, and need not meet the stringent standards for prior restraints, because posting encryption source code on the Internet "is not an activity that is 'commonly associated with expression.'" 8 F. Supp. 2d at 718. But that ignores the court's own findings that encryption source code texts express ideas that are understood by trained readers. *See* Part I, pp. 6-14, above. The Regulations are plainly directed specifically at expression of this subject. *See Bernstein III*, 974 F. Supp. at 1305. The District Court's conclusion here also flies in the face of the Supreme Court's recent decision in *Reno v. ACLU,* in which the Court declared, "[t]he Internet is a 'unique and wholly new medium of worldwide human communication.'" 117 S. Ct. at 2334.

> '[T]he content on the Internet is as diverse as human thought.' . . . [O]ur cases provide no basis for qualifying

> the level of First Amendment scrutiny that should be applied to this medium.

Id. at 2335, 2344.

There is no foundation for the District Court's suggestion that the Regulations' prior restraints are not directed at expression because *certain* encryption information may be disseminated in *certain* media, such as publicly available books. *See* 8 F. Supp. 2d at 718-19. A prior restraint on one medium — for instance, sound recordings or films — cannot be saved from First Amendment scrutiny merely because no similar prior restraint is imposed on printed material. As the Supreme Court explained in *Reno v. ACLU*,

> The Government's position is equivalent to arguing that a statute could ban leaflets on certain subjects as long as individuals are free to publish books. In invalidating a number of laws that banned leafleting on the streets regardless of their content, we explained that "one is not to have the exercise of his liberty of expression in appropriate places abridged on the plea that it may be exercised in some other place."

117 S. Ct. at 2348-49. Thus a prior restraint on Internet publication or electronic dissemination cannot avoid the First Amendment simply because the restraint does not apply to some printed material.

The District Court also erred in its view that the pre-publication licensing requirements for source code texts are not subject to prior restraint scrutiny because the Regulations impose the same treatment on encryption devices. *See* 8 F. Supp. 2d at 718. Content-based prior restraints on expression cannot be insulated from the First Amendment by imposing similar restraints on non-expression. *See, e.g., Vance v. Universal Amusement Co.*, 445 U.S. 308, 100 S. Ct. 1156 (1980) (striking down statute regulating gambling, prostitution, and bull fighting, in addition to obscenity).

B. The Regulations' prior restraint is also unconstitutional because it fails to provide procedural safeguards.

The Regulations embody a prior restraint that is unconstitutional for a second, independent reason: The statutory scheme lacks the fundamental procedural safeguards that the Supreme Court has identified as essential to a government licensing scheme. *See, e.g., FW/PBS v. Dallas,* 493 U.S. 215 (1990); *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 the following two procedural safeguards: There must be definite and reasonable limitations on the time for the licensing decision; and expeditious judicial review

of the licensing decision must be available. *See Freedman v. Maryland, 380 U.S. 51, 58-59 (1965); FW/PBS*, 493 U.S. at 227-30*; United States v. Thirty-Seven Photographs*, 402 U.S. 363, 374 (1971). The Regulations fail in both respects. First, they impose no time limits at all on the government's licensing determinations.[2] Second, the Regulations do not provide prompt judicial review of the government's licensing decision: Indeed, the government apparently takes the position that judicial review is not available at all for licensing decisions under the Regulations. *See* 15 C.F.R. §756.2(c). The Supreme Court has repeatedly emphasized the importance of the availability of expeditious judicial review of licensing determinations. *See, e.g.*, *Freedman* 380 U.S. at 58-59; *Thirty-Seven Photographs*, 402 U.S. at 368.

The District Court suggests erroneously that these procedural safeguards are not required for restraints that are not narrowly directed at expression or expressive conduct. *See* 8 F. Supp. 2d at 719. The Supreme Court concluded in *FW/PBS* that the above procedural safeguards must be provided in

[2] A nominal 90-day deadline for an initial decision may be tolled by a variety of circumstances or government actions, including referral to the President, and there is no time limit for final agency action. *See* 15 C.F.R. §§ 750.4(a)(1), 756.2(c)(2).

any system of prior restraint, *regardless* of whether it is content-neutral or content-based. 493 U.S. at 227-30; *see also Lakewood v. Plain Dealer Publishing Co.*, 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."); *East Brooks Books, Inc. v. City of Memphis*, 48 F.3d 220, 224 (6th Cir. 1995). Whether or not the Regulations were specifically *intended* to prevent exchange of information or ideas, regulations with the *effect* of restraining expression prior to its publication are subject to prior restraint scrutiny. *See Lakewood*, 486 U.S. at 770.

The Regulations in this case are therefore subject to the established procedural requirements for prior restraints, even assuming *arguendo* that they are content-neutral, and their failure to conform to those requirements renders them unconstitutional.

III. The Regulations Constitute an Unconstitutional Content-Based Regulation of 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. *Boos v. Barry*, 485 U.S. 312 (1988).

A. The Regulations distinguish encryption source code from other source code text, and restrict its international and Internet publication, based solely on its cryptographic content.

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. It is undisputed that if the source code at issue embodied word processing algorithms, for example, instead of encryption algorithms, the Regulations would not restrict its dissemination. The District Court expressly recognized that the Regulations distinguish encryption software from all other software and impose more onerous restrictions based solely on the software's encryption content: The Regulations "subject encryption software to heightened licensing regulations that do not apply to other types of software," the court held. "[A]ll]types of software are regulated as 'technology' [*i.e.*, information] . . . [but] encryption software is categorized under the stricter 'commodity' standard." 8 F. Supp. 2d at 720 (citations omitted). 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 source code text based solely on its content.

A government regulation that restricts expression based on its content or subject matter is unconstitutional, absent a compelling governmental interest and narrow tailoring of means to end. *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, 95 (1972) ("[A]bove all else, the First Amendment means that government has no power to restrict expression because of its . . . subject matter, or its content.").

B. The District Court erred by ignoring the Regulations' content-based distinction and ruling that the challenged restrictions are content-neutral.

The District Court ruled erroneously that the Regulations are content-neutral, despite the acknowledged fact that software with encryption content is singled out for pre-publication licensing.

The District Court erred first by declaring that regulations cannot be considered content-based unless they are motivated by the government's express disagreement with the message. No such illicit government intent is required to demonstrate that a regulation is subject to strict scrutiny as a content-based

restriction. The Supreme Court has rejected the notion that First Amendment analysis requires courts to peer into the subjective minds of officials:

> 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.

Minneapolis Star & Tribune Co. v. Minnesota Comm'r of Revenue, 460 U.S. 575, 592 (1983) (citations omitted).

Second, although the District Court plainly recognized that source code and software with encryption content are singled out for onerous burdens, *see* 8 F. Supp. 2d at 722, it nevertheless concluded that the burdens are not content-based because of the functional characteristics of the software. But mathematical formulae, musical scores and technical instructions are just as functional (and just as expressive) as source code text. If the government selectively suppressed mathematical formulae or technical information on a particular subject, it could not escape the strict scrutiny that is due to content-based suppression simply by asserting that the formulae or information are "inherently functional."

The court also suggests that encryption software is validly regulated, whereas books containing source code are not, because electronically-stored source

code is more functional than paper-based code. 8 F. Supp. 2d at 720-21. The difference between encryption source code stored on disk rather than printed in a book has no constitutional significance. It is a trivial matter to convert the printed source code to electronic form by typing or scanning the text into a computer. The minimal incremental increase in functionality offered by the electronic form as compared with printed media cannot justify its suppression.

Finally, the District Court also erred by concluding that the Regulations are content-neutral because they "do not attempt to restrict the free flow of public information and ideas about cryptography." 8 F. Supp. 2d at 720. There is no dispute that the Regulations are specifically intended to, and do, restrict the free flow of encryption source code via the Internet or electronic publication based solely upon the encryption content. *See* 8 F. Supp. 2d at 713. All other kinds of information, including source code, may be freely disseminated by these media; only encryption is suppressed. Yet the Supreme Court has made clear that publication on the Internet and by electronic means enjoys full protection of the First Amendment. *Reno v. ACLU*, 117 S. Ct. at 2344. The Supreme Court thus rejected any claim that the government could bar Internet publication of certain

materials simply because the government did not attempt to restrict the "free flow" of such materials in printed media.

C. Even if the Regulations were not subject to strict scrutiny, they are unconstitutional because they are not narrowly tailored and do not provide adequate alternative channels of communication.

For the reasons stated, the District Court erred by finding that the Regulations are content-neutral, and thus subject only to the intermediate scrutiny test outlined in *United States v. O'Brien*, 391 U.S. 367, 377 (1968), for conduct with expressive elements. *See* 8 F. Supp. 2d at 72. Even if the court were correct in adopting that standard, however, the Regulations still could not pass constitutional muster.

Under the *O'Brien* standard, the pre-publication licensing scheme can be justified only if it furthers an important government interest; is unrelated to the suppression of free expression; and the "incidental" restriction is narrowly tailored — *i.e.*, no greater than is "essential" to further the government's interests. 391 U.S. at 377. In addition, when the restriction forecloses an entire medium of expression to a certain type of speech, the regulation must "leave open ample alternative channels for communication." *City of Ladue v. Gilleo*, 512 U.S. 43, 56

(1994) (quoting *Clark v. Community for Creative Non-Violence*, 468 U.S. 288, 293 (1984)); *see also Reno v. ACLU*, 117 S. Ct. at 2348-49.

National security is an important governmental interest. But even assuming *arguendo* that the Regulations are not related to suppression of expression, they nonetheless are not tailored narrowly to achieve the government's stated purpose, nor do they provide adequate alternative channels for communication.

Speech-restrictive regulations that fail to accomplish their stated purpose to any significant degree cannot be found to be narrowly tailored. *See, e.g.*, *City of Ladue*, 512 U.S. at 52. The Regulations aim to prevent encryption software, including source code, from falling into the hands of foreigners hostile to the United States. But the record shows that those overseas and hostile to the United States are able to obtain comparable software from foreign sources or by downloading nearly identical software from one of many Internet sites. Stipulation ¶ 25. Moreover, there is no dispute that encryption source code may be published in books abroad. Thus, foreign groups hostile to the United States can avail themselves of American-made encryption code simply by typing or scanning the printed source code into electronic form. The Regulations fall too far short of their

stated purpose to be found narrowly tailored and cannot survive even intermediate constitutional scrutiny.

Furthermore, the Regulations do not offer adequate alternative channels of communication. The Supreme Court has warned against the danger of shutting off any unique and important means of communication:

> [T]he Court long has recognized that by limiting the availability of particular means of communication, content-neutral restrictions can significantly impair the ability of individuals to communicate their views to others . . . To ensure the widest possible dissemination of information . . . the First Amendment prohibits not only content-based restrictions that censor particular points of view, but also content-neutral restrictions that unduly constrict the opportunities for free expression.

City of Ladue, 512 U.S. at 55 n.13 (quoting Geoffrey R. Stone, *Content-Neutral Restrictions*, 54 U. Chi. L. Rev. 46, 57-58 (1987)) (citations omitted); *see also Reno v. ACLU*, 117 S. Ct. at 2348-49.

The practical effect — indeed, an explicit goal — of the Regulations is to eliminate the Internet as a medium of communication for encryption software, including source code. Print media are poor substitutes for the fast-moving, interactive Internet. Academic discourse in recent years has moved away from print media into the world of Internet communications, and the Internet is

particularly vital for scientists and professors in the field of computer programming. An academician may wait a year or more to see an article published in print; by contrast, the Internet offers scholars and scientists the opportunity to post their work and invite immediate comment. The work of a scientist confined to print may well be obsolete by the time it is disseminated. The Regulations prevent American scholars and scientists from taking part in this discourse, not only with those abroad, but also among themselves. "To impose any straight jacket upon the intellectual leaders in our colleges and universities would imperil the future of our Nation." *Sweezy v. New Hampshire*, 354 U.S. 234, 250 (1957).

IV. The Regulations Burden Private Speech.

Encryption is also critical to safeguard the right of private speech, which implicates important First and Fourth Amendment values. The Regulations on cryptographic software have the effect of controlling the result — private speech — by controlling the tools necessary to achieve that result in the electronic sphere. The government cannot target the tools of expression in order to restrain or burden the underlying expression itself. *See, e.g., Minneapolis Star*, 460 U.S. at 585. The Regulations chill private electronic communications, impermissibly

burden constitutionally protected speech, and interfere with people's reasonable expectation of privacy in their electronic communications.

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

Governmental regulation of the free flow of encryption information and software endangers personal privacy. Encryption can protect 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.

Moreover, encryption has become a vital tool for human rights activists and political dissidents throughout the world for confidential

communications free from intrusion. *Amicus* Human Rights Watch increasingly needs encryption for its communications with human rights activists. Its staff regularly encrypts eye-witness reports and communications gathered from around the globe in situations where victims of serious abuse may still be vulnerable to reprisals. *See also* David Banisar, *A Primer on Electronic Surveillance for Human Rights Organizations*, International Privacy Bulletin (July 1993).

Governmental restrictions on the export of encryption software impede the development of the secure global infrastructure that electronic privacy requires. The Regulations substantially constrain communications over 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 also have a negative impact on the development and availability of effective encryption software even within the United States. *See* National Research Council, *Cryptography's Role in Securing the Information Society*, §4.3.1 (National Academy Press 1996) ("*NRC Report*"). For example, some U.S. software developers have elected to produce only software, particularly word processing and spreadsheet software, with relatively ineffective encryption features that are not subject to the Regulations' restrictions.

Individuals will increasingly demand that their personal privacy be preserved, and commercial entities will require the highest level of protection for valuable financial and proprietary data. The demand for security must be met, if not by U.S. 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*, §4.4.2.

B. Private communications are protected by the convergence of First and Fourth Amendment values.

The mechanisms that secured traditional paper-based communications — envelopes and locked filing cabinets — are being replaced by cryptographic security techniques. To require that electronic communications and records be unencrypted is equivalent to requiring that paper communications be sent by postcards instead of 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.

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. *United States v. United States District Court*, 407 U.S. 297, 313 (1972) ("*Keith*"). The Fourth Amendment shields private communications from unreasonable governmental interference or surveillance. *See, e.g., Keith*, 407 U.S. 297*; Katz v. United States*, 389 U.S. 347 (1967). In particular, "governmental incursions into conversational privacy" via electronic means "necessitate the application of Fourth Amendment safeguards." *Keith*, 407 U.S. at 313; *see also 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.").

Courts have recognized that those who use the Internet and other electronic communications have come to expect that their communications, and often their identities, will remain private. *See, e.g., United States v. Maxwell*, 45 M.J. 406 (C.A.A.F. 1996) (reasonable expectation of privacy in electronic communications); *ACLU v. Reno*, 929 F. Supp. 824, 849 (E.D. Pa. 1996), *aff'd*,

117 S. Ct. 2329 (1997) (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*, 977 F. Supp. 1228, 1356 (N.D. Ga. 1997) (finding substantial likelihood that statute compelling identity of Internet communicant was unconstitutional).

Without readily available encryption software, however, electronic communications can be easily intercepted, and communications intended to be private may be 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 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." 969 F. Supp. 160, 165 (S.D.N.Y. 1997).

In sum, the Regulations 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. The District Court did not, and could not, find such a compelling government interest here.

CONCLUSION

For the reasons stated above, the District Court's judgment should be reversed.

Respectfully submitted,

_____

Kurt A. Wimmer
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., S.E.
Washington, DC 20003
(202) 544-9240

Counsel for *Amici Curiae*

Date: March 8, 1999

CERTIFICATE OF COMPLIANCE

I hereby certify that this Brief of *Amici Curiae* complies with the type-volume limitations of Fed. R. App. P. 29(d) and 32(a)(7)(B), and that the word processor used to prepare the brief reports that the relevant portions of the brief contain 6,698 words.

_____

David W. Addis
COVINGTON & BURLING
1201 Pennsylvania Ave., N.W.
P.O. Box 7566
Washington, DC 20044

Counsel for *Amici Curiae*

CERTIFICATE OF SERVICE

I hereby certify that I have, this 8th day of March 1999, arranged to send by overnight courier two copies of the foregoing Brief of *Amici Curiae* to:

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

Gino J. Scarselli, Esq.
ACLU of Ohio Foundation, Inc.
1266 W. 6th Street, Suite 200
Cleveland, OH 44113

J. Joshua Wheeler, Esq.
The Thomas Jefferson Center for the Protection of Free Expression
400 Peter Jefferson Place
Charlottesville, VA 22911

_____

David W. Addis
COVINGTON & BURLING
1201 Pennsylvania Ave., N.W.
P.O. Box 7566
Washington, DC 20044

Counsel for *Amici Curiae*