Govt. Appeal Reply, November 20, 1997, in Bernstein v. Commerce

This is a series of page images from a fax machine.

If you want to view or print it in pieces, here are the first ten pages, and next ten pages, and next ten pages, and next ten pages, and of the motion. You can also download the individual image files, named "page01.gif", "page02.gif", etc. (1 through 38).

No. 97-16686

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

DANIEL J. BERNSTEIN,

Plaintiff-Appellee,

v.

U.S. DEPARTMENT OF COMMERCE, et al.,

Defendants-Appellants.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

REPLY BRIEF FOR THE APPELLANTS

FRANK W. HUNGER
Assistant Attorney General

MICHAEL J. YAMAGUCHI
United States Attorney

STEPHEN W. PRESTON
Deputy Assistant Attorney General

DOUGLAS N. LETTER
SCOTT R. McINTOSH
Attorneys, Appellate Staff
Civil Division, Room 9550
Department of Justice
601 D Street, N.W.
Washington, D.C. 20530-0001

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Constitution:

Statutes:

Regulations:

Orders:

Miscellaneous:

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

No. 97-16686

DANIEL J. BERNSTEIN,

Plaintiff-Appellee,

v.

U.S. DEPARTMENT OF COMMERCE, et al.,

Defendants-Appellants.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

REPLY BRIEF FOR THE APPELLANTS

ARGUMENT

I. Introduction

A. Professor Bernstein's brief paints an alarming portrait of the EAR's encryption export controls as an engine of government censorship. According to Bernstein, the export provisions are "aimed at an entire subject area of science," the "subject [of] cryptography" (Brief 1, 4). The EAR is claimed to single out the "topic

of encryption" for more restrictive treatment than other "scientific topics" subject to the EAR (id. at 11). In Bernstein's account, the government uses the EAR to engage in ongoing "[c]ensorship of academic speech about cryptography" (id. at 7). The EAR's export controls "prevent Professor Bernstein and many other academics and scientists from effectively teaching and publishing about the mathematical field of cryptography" (id. at 16). Remarkably, the government persists in this enterprise despite the fact that the Department of Justice "has known for 20 years that these regulations are an unconstitutional prior restraint" (id. at 3).

This account is dramatic, but it is wrong -- wrong in fact and wrong in law. Bernstein's constitutional arguments rest on a fundamentally inaccurate depiction of what the EAR's encryption export provisions are and what they do. Before we turn to the details of Bernstein's First Amendment claims, it is therefore important to clarify the nature of the regulatory scheme that this Court has before it.

Contrary to Bernstein's repeated suggestions, the EAR does not purport to control the "topic of encryption" or "speech about cryptography." The regulations at issue in this case are directed at the export of products that encrypt data, not at the "topic" of cryptography. See 15 C.F.R. 742.15. The regulations do not require a license for the public dissemination or export of information and ideas about

cryptography. See id. § 734.3(b)(3), 734.7-734.9; Brief for the Appellants (hereafter "Government Brief") 29-30.[1] Nor do they require a license for the export of books and magazines devoted in whole or in part to cryptographic subjects, even if the publications contain encryption source code in printed form. See id. § 734.3(b)(2) and Note following § 734.3(b)(3). The regulations therefore simply do not place the government in a position to decide what may and may not be publicly taught or discussed, either domestically or abroad, about the subject of cryptography.

For present purposes, what is noteworthy about the EAR is how little, rather than how much, it affects Bernstein's academic endeavors. Bernstein does not need a license under the EAR to engage in public discussions and instruction about cryptography in the classroom or in academic conferences, either here or abroad. See 15 C.F.R. 734.3(b)(3), 734.7(a)(4), 734.9, 744.9; Government Brief 48-50. Nor does he need a license to distribute copies of his encryption program to his students -- or to anyone else in this country, for that matter, other than an agent of a foreign

[1] Bernstein is therefore flatly wrong when he asserts (at 9) that a license is required not only for the electronic export of encryption software, but also for the electronic export of encryption technology. Publicly available technology is simply outside the scope of the EAR (see 15 C.F.R. 734.3(b)(3)) and therefore publicly available encryption technology may be exported without a license by electronic means or in any other medium.

government. See 15 C.F.R. 734.2(b)(9)(i)(B); Government Brief 50 n.19. He does not need a license to distribute his ideas about cryptography abroad in books, journals, or other print media, even if the source code for his encryption program is itself printed in such publications. 15 C.F.R. 734.3(b)(2); Government Brief 10.[2] And despite his insistence that the EAR excludes him from "publishing" his encryption program electronically, he does not even need a license to distribute his program via the Internet, as long as he takes adequate precautions to prevent the unauthorized transfer of the program outside the United States. 15 C.F.R. 734.2(b)(9)(ii). For example, Bernstein is free to distribute his program to domestic recipients by electronic mail, and he can make the program publicly available on a World Wide Web site that is configured to exclude foreign access. Id. § 734.2(b)(9)(ii)(A)-(B).[3]

---

[2] Bernstein is therefore wrong when he claims (at 18) that he needs a license to "take or send Snuffle 5.0 abroad in any manner" or to "present Snuffle 5.0 at a conference abroad or communicate it privately to an overseas colleague." He is perfectly free to distribute printed materials reproducing his source code to his foreign colleagues for academic purposes. He may do so either in person (for example, at a foreign academic conference) or by mail. The EAR therefore bears no resemblance to Bernstein's hypothetical regulation "prevent[ing] composers from exchanging sheet music" (31).

[3] For example, Microsoft Corporation makes Web "browser" software containing (continued...)

Because the EAR's provisions are designed not to prevent the free public exchange of information and ideas about cryptography, it is hardly surprising that academic discourse about cryptography is flourishing. As noted in our opening brief, the record below shows that cryptography is the subject of numerous college courses, academic symposia, textbooks, and fundamental research published in scholarly journals. See ER 108-297, 305-419. Indeed, Bernstein himself acknowledges (at 28) that "articles and papers containing and discussing cryptographic algorithms, source code[,] and theories have been published in scientific journals for over 25 years for peer review and evaluation." None of this academic activity requires government approval, permission, or review.

In the face of this record, Bernstein insists (at 7) that the government is engaging in "censorship of academic speech about cryptography." But the record materials that Bernstein cites (at 7-8) as evidence of this supposed "censorship" do not even begin to support Bernstein's characterization.

---

[3](...continued)
strong (128-bit) encryption capabilities available for domestic downloading from its Web site (http://www.microsoft.com/ie/download/?/ie/download/128bit.htm) pursuant to this provision.

For example, Bernstein cites (at 7) a declaration from Peter Junger, a law professor at Case Western Reserve University, as evidence that "licenses are required for academic activities involving cryptography." Junger contacted the Department of State and the Department of Commerce to inquire about the applicability of export controls to an encryption program that he had created. AER 174-75. According to Junger himself, he was told that "discussing the program in class should not cause a problem." Id. at 175 (emphasis added). Junger nevertheless chose not to disclose his encryption program or cryptographic information in his classroom or other academic settings where foreigners were present. Junger believed that such disclosures would require an export license. Id. at 177-78. That belief was wrong then, and as explained above, it is equally wrong now. A regulatory scheme that does not require a license for academic instruction can hardly be condemned because of someone's misimpression that it does.

Bernstein is equally wrong when he claims (at 3) that the Department of Justice has found the EAR's encryption software export provisions to be unconstitutional. Bernstein points to memoranda prepared by the Department's Office of Legal Counsel (OLC) nearly two decades ago regarding the terms of export regulations then administered by the Department of State. However, the regulations in question there

did not involve encryption software, the subject of the district court's First Amendment ruling in this case. Instead, they involved "technical data" -- information about how to create and use encryption products, the kind of information that the EAR refers to as "technology" (see Government Brief 10). By its terms, OLC's First Amendment analysis was directed at the controls on the export of technical data and did not question the controls on the export of encryption software or other encryption products. See, e.g., Appellee's Excerpts of Record (AER) 241 (distinguishing between "[c]ryptographic devices" and "technical data"). Here, as elsewhere in his brief, Bernstein simply ignores the regulatory distinction between encryption products and cryptographic information -- a distinction that is critical to the resolution of the First Amendment issues in this case.

In addition, Bernstein fails to note that the regulations addressed in the OLC memoranda were subsequently changed in numerous respects to meet the concerns expressed by OLC and the First Amendment reasoning of this Court in United States v. Edler Industries, 579 F.2d 516 (9th Cir. 1978). See 49 Fed. Reg. 47682, 47683, 47685-86 (Dec. 6, 1984); 56 Fed. Reg. 44548 (Oct. 28, 1991); 58 Fed. Reg. 39285 (July 22, 1993). In particular, the regulations were modified to eliminate any licensing requirement for the dissemination of publicly available information,

including information resulting from academic research. See 22 C.F.R. 120.10(a)(5), 120.11.[4] The EAR carries forward these changes in its provisions regarding encryption technology and technical assistance. See 15 C.F.R. 734.7-734.9, 744.9(a). Those provisions are therefore entirely consistent with the views regarding the First Amendment expressed in the OLC memoranda.

B. Bernstein's mischaracterization of the nature and operation of the EAR, and his unwillingness to acknowledge the distinctions that the EAR draws between encryption products and cryptographic information, reflect his resolutely one-sided view of the product that lies at the heart of this case -- encryption software in source code form. The underlying premise of Bernstein's brief is that because encryption source code is capable of being used to represent and convey cryptographic ideas, it is no different for First Amendment purposes than any other kind of "information" about cryptography. But as we explained at length in our opening brief, encryption source code is fundamentally different from mere cryptographic "information," precisely because it is not merely "information": it is capable of carrying out the

---

[4] Bernstein cites (at 6-7) instances in the early 1980s, at the beginning of the first Reagan Administration, when the government allegedly sought to restrict academic discussions of cryptography. Even if Bernstein's characterization of these episodes is taken at face value, all of them predate the regulatory amendments cited above.

physical task of controlling the operation of a computer, and it can do so without conveying any information or ideas about cryptography to the person who is using it. See Government Brief 27-28. It is this wholly non-informational capability that underlies the controls that the President has placed on the export of all products -- software and hardware alike -- that can be used to encrypt data.

The First Amendment issues in this case cannot be disposed of, as Bernstein would prefer, simply by labeling encryption source code as "information" or "speech." What is required is a more thoughtful First Amendment analysis, one that acknowledges not only the potential for encryption source code to represent cryptographic information, but also its entirely non-informational capacity to control the physical operation of computers in ways that can compromise this country's national security and foreign policy interests. We turn to that analysis now.

II. The EAR's Export Controls Are Not a Facially Unconstitutional Prior Restraint

A. Bernstein urges this Court to hold that the EAR's encryption export controls are facially unconstitutional under the prior restraint doctrine -- to hold, in other words, that the risk of censorship of ideas or viewpoints is so ingrained in these regulations that the regulatory scheme must be invalidated on its face without a

showing that the government has actually employed it to suppress disfavored speech in any particular case. However, City of Lakewood v. Plain Dealer Publishing Co., 486 U.S. 750 (1988), holds that "laws of general application that are not aimed at conduct commonly associated with expression" are not subject to facial invalidation under the prior restraint doctrine, but rather may be challenged only on an as-applied basis. Under Lakewood, "a facial freedom of speech attack must fail unless, at a minimum, the challenged statute 'is directed narrowly and specifically at expression or conduct commonly associated with expression.'" Roulette v. City of Seattle, 97 F.3d 300, 305 (9th Cir. 1996) (emphasis added) (quoting Lakewood, 486 U.S. at 760).

Bernstein argues that the EAR's encryption export controls have a sufficient "nexus" to expression to support a facial challenge because they apply to activities, such as the posting of encryption source code on Internet "newsgroup" sites, that can be undertaken for academic or informational purposes. But as we explained in our opening brief (at 41-42), the bare fact that a general licensing scheme happens to encompass activities that can (but need not) be undertaken for expressive purposes is not enough to subject it to facial challenge under Lakewood. A facial challenge is permissible only when the licensing scheme singles out expression or expressive

activity -- when it "'is directed narrowly and specifically at expression or conduct commonly associated with expression.'" Roulette, 97 F.3d at 305 (emphasis added).

The provisions at issue here simply do not single out expression or expressive activities in this fashion. They encompass all encryption products -- hardware as well as software, object code as well as source code. They draw no distinction among these products based on their potential, or lack of potential, to convey information and ideas about cryptography. The conduct involving these products that the government regulates is not "publishing," as Bernstein would have it, but rather the exporting of encryption products. The fact that this regulated conduct could be undertaken for expressive purposes in a particular case does not mean that the export controls "focus directly" on "an important form of academic and scientific communication" (Bernstein Brief 26), any more than a law requiring commercial building permits "focuses directly" on an "important form" of speech because it happens to cover the construction of newspaper facilities. See Lakewood, 486 U.S. at 761. Nor does it mean that these regulations create a sufficiently "real and substantial threat" of censorship (Lakewood, 486 U.S. at 759) to warrant facial invalidation. Cf. Jones Intercable of San Diego, Inc. v. City of Chula Vista, 80 F.3d 320, 325 (9th Cir. 1996) (declining to entertain facial challenge to regulation that

"applies to conduct as well as speech, and encompasses many potential activities having no expressive function").

B. Bernstein also argues (at 39-40) that the prior restraint doctrine requires the government to meet the "substantive" standards of the Pentagon Papers case, New York Times Co. v. United States, 403 U.S. 713 (1971) (per curiam), by "proving" that "publication" of encryption source code would "'surely result in direct, immediate, and irreparable damage'" to this country. But as we explained in our opening brief (at 37-38), the Pentagon Papers case is simply irrelevant here. The government's object in the Pentagon Papers case was to suppress "'information whose disclosure would endanger the national security.'" 403 U.S. at 718 (Black, J., concurring) (quoting government brief); id. at 726 n.* (Brennan, J., concurring). The use of a prior restraint to prevent speakers from communicating disfavored information and ideas to the public strikes at the heart of the First Amendment, and for that reason, an exceptionally compelling showing by the government is required to justify such an undertaking. In contrast, when a regulatory scheme is not designed to suppress disfavored information and ideas, the mere fact that it involves licensing does not subject it to the kind of strict scrutiny employed in the Pentagon Papers case.

Bernstein insists (at 41) that this case is indistinguishable from the Pentagon Papers case because the government's ultimate concern in both cases is national security. Here, as elsewhere, Bernstein ignores the wholly non-informational nature of the risks posed by encryption software. The threat to national security comes not from any cryptographic ideas that encryption software may be claimed to convey, but instead from its capacity to make computers encrypt data -- a physical capacity that does not depend in any way on the ability of the software's recipient to "read" it or to use the "information" about cryptography that the program may embody. Because the government manifestly is not attempting to further national security by preventing the disclosure of information and ideas, and because (as explained above) the regulatory scheme goes out of its way not to require a license for the public dissemination and export of cryptographic information, the Pentagon Papers Case remains irrelevant.

III. The EAR's Export Controls Satisfy The First Amendment Standards Governing Content-Neutral Regulations

A. We now turn from the prior restraint doctrine to the issue of content neutrality. At the outset, we wish to dispel any possible confusion about the relationship between these two issues.

Bernstein asserts (at 21) that we are presenting content neutrality as a way to "bypass" prior restraint analysis. Bernstein evidently understands us to be arguing that, if government regulations are content neutral, they are not subject to a facial challenge on prior restraint grounds. As the foregoing discussion of the prior restraint doctrine should make clear, however, that is not our position. Bernstein's facial prior restraint claim fails under Lakewood for other reasons -- in particular, because the EAR's export controls are not "directed narrowly and specifically at expression or conduct commonly associated with expression'" (Roulette, 97 F.3d at 305).

B. For First Amendment purposes, "[t]he test [of content neutrality] is whether the government has adopted the restriction 'because of disagreement with the message [the speech] conveys.'" One World One Family Now v. City and County of Honolulu, 76 F.3d 1009, 1012 (9th Cir.), cert. denied, 117 S. Ct. 554 (1996) (quoting Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989)). In our opening brief (at 25-30), we demonstrated that, under this standard, the EAR's controls on the export of encryption software are manifestly "unrelated to the content of speech." Turner Broadcasting System, Inc. v. FCC, 512 U.S. 622, 642 (1994).[5]

[5] Indeed, this is an even clearer case for application of the intermediate standard for content-neutral regulations than cases such as Ward and One World One Family (continued...)

Bernstein argues (at 21-22) that the EAR is not neutral on "the subject of cryptography" because it treats encryption software differently from other software in certain respects (see Government Brief 12-14). But as we have already explained at length, the EAR's encryption software provisions are not directed at "the subject of cryptography" at all; they are directed at products that make computers encrypt data. To the extent that the EAR treats encryption software differently from other software, it is solely because of the physical capacity of encryption software to make computers encrypt data, not because of any conceivable "'disagreement with the message'" (One World, 76 F.3d at 1012) that encryption source code may be claimed to convey. See Government Brief 12. It is the government's concern with the non-informational, physical capacity of encryption software to control computers that explains why the EAR treats encryption software (including source code) just like encryption hardware. See Executive Order 13206, 61 Fed. Reg. 58768 (Nov. 19, 1996); 15 C.F.R. 742.15; Government Brief 12-13.

---

[5](...continued)
Now, since, as explained in our discussion of the prior restraint doctrine, the reach of the EAR is not confined to communicative activities. Instead, the export controls are "aimed at regulable conduct and hav[e] only an incidental impact on speech." Clark v. CCNV, 468 U.S. 288, 298 n.8 (1984).

By way of analogy, one can readily imagine a law imposing special restrictions on the distribution or export of computer "virus" software because of the capacity of computer viruses to damage electronic data. Cf. 18 U.S.C. 1030(a)(5)(A) (unlawful to "knowingly cause[] the transmission of a program * * * and [thereby] intentionally cause[] damage[,] without authorization, to a protected computer"). The fact that such a law would treat computer virus software more restrictively than other software would hardly mean that, for First Amendment purposes, the restrictions were a content-based regulation of "the subject of computer viruses" or "speech about viruses."

Bernstein argues (at 30) that the government's focus on the capacity of encryption source code to make computers encrypt data is misplaced because "most speech," such as political speech and parody, "has the 'capacity' to do something." But the "capacity" of political speech or parody to "do something" is entirely a product of the information and ideas that such speech conveys. Political speech unquestionably has "the capacity to spur people to vote or to protest," as Bernstein notes (at 30), and parody has "the capacity to inflict emotional distress" (ibid.), but they cause these reactions because (and only because) people understand and react to the ideas that they convey. In contrast, as explained our opening brief, the capacity

of encryption source code to make a computer encrypt data does not depend on whether the user understands, or is even capable of understanding, the "ideas" embodied in the source code itself. See Government Brief 27-28. Like the district court's misconceived analogies to "how-to books" and recipes (ibid.), Bernstein's analogies to political speech and parody ignore this critical distinction.

Bernstein's reliance on cases like Brandenburg v. Ohio, 395 U.S. 444 (1969) (per curiam), and American Booksellers Ass'n v. Hudnut, 771 F.2d 323 (7th Cir. 1985), aff'd mem., 475 U.S. 1001 (1986), is misplaced for the same reason. These cases reflect the general principle that the government cannot suppress speech merely because the information and ideas that it conveys are "dangerous." See Brandenburg, 395 U.S. at 447-49; Hudnut, 771 F.2d at 327-30. If the EAR's export controls were intended to protect against the "danger" posed by cryptographic ideas, these precedents might have some relevance, but the dangers at issue here have nothing to do with ideas.

Contrary to Bernstein's suggestion (at 28 n.34), the government is not proposing "a First Amendment exception" for "speech which can also be used to control a machine." We are not proposing an "exception" to the First Amendment at all. Instead, we are simply relying on the long-established First Amendment

distinction between laws that "suppress, disadvantage, or impose differential burdens on speech because of its content" (Turner Broadcasting System, Inc. v. FCC, 512 U.S. 622, 642 (1994)) and laws that are "'justified without reference to the content of the regulated speech'" (Ward, 491 U.S. at 791) (emphasis in original).

C. Bernstein asserts (at 29) that even if the justification for the EAR's export controls is unrelated to the content of speech, "[w]here, as here, government action directly restricts protected speech, the government's good intentions are irrelevant." But the EAR's encryption export controls do not "directly restrict" protected speech, any more than the government was "directly restricting" protected speech in United States v. O'Brien, 391 U.S. 367 (1968), when it criminally prosecuted a person who burned his draft card to protest the Vietnam War; in Ward, where the government imposed restrictions on the volume of music at outdoor concerts; or in Turner, where the government required cable operators to carry broadcast television programming. To the extent that any of these restrictions affect "protected speech," they do so only incidentally, as an unsought consequence of the government's pursuit of goals that are unrelated to the suppression of ideas. The whole point of the Supreme Court's precedents is that this kind of incidental effect neither invalidates such laws nor subjects them to strict scrutiny under the First Amendment.

Bernstein also cites Minneapolis Star & Tribune Co. v. Minnesota Comm'r of Revenue, 460 U.S. 575, 592 (1983), for the proposition that "illicit legislative intent is not the sine qua non of a First Amendment violation." That is perfectly true. But it hardly follows, as Bernstein suggests, that the absence of "illicit legislative intent" is irrelevant. When a regulatory scheme is not the product of an intent to suppress speech because of disagreement with what it says, the Supreme Court's content-neutrality precedents supply the governing First Amendment standards.

D. Once it is recognized that the justification for the EAR's encryption export controls is unrelated to the content of speech, the First Amendment inquiry turns to whether the controls "'further[] an important or substantial governmental interest.'" Turner, 512 U.S. at 662; see Government Brief 30.[6] Here, Bernstein does not question the President's determination that the use of strong encryption products abroad can seriously compromise this country's national security and foreign policy interests. 32 Weekly Comp. Pres. Doc. 2397 (Nov. 15, 1996) (Presidential memorandum); see also ER 96 (Deputy Director of NSA). However, he disagrees

---

[6] This inquiry is not confined, as amicus American Association for the Advancement of Science suggests (at 15-22), to cases involving regulations of "conduct" or "time, place, and manner" regulations. Instead, as the Supreme Court's decision in Turner makes clear, it applies whenever the justification for a challenged regulation is unrelated to the content of speech. See Government Brief 24-25, 30-31.

with the President regarding the value of the EAR's export controls as a means of avoiding these harms. He argues that the export controls are futile (1) because the EAR does not restrict the export of printed materials that contain encryption source code and (2) because encryption software programs are available abroad.

In inviting this Court to second-guess the President's judgments about the efficacy of the export controls, Bernstein ignores the basic unsuitability of the judicial process to such an undertaking. As the Supreme Court explained in Chicago & Southern Air Lines v. Waterman Steamship Corp., 333 U.S. 103, 111 (1948) (emphasis added):

> [T]he very nature of executive decisions as to foreign policy is political, not judicial. Such decisions are wholly confided by our Constitution to the political departments of the government, Executive and Legislative. They are delicate, complex, and involve large elements of prophecy. They are and should be undertaken only by those directly responsible to the people whose welfare they advance or imperil. They are decisions of a kind for which the Judiciary has neither aptitude, facilities nor responsibility and have long been held to belong in the domain of political power not subject to judicial intrusion or inquiry.

This Court has already recognized the force of these considerations with regard to the EAR. In United States v. Mandel, 914 F.2d 1215 (9th Cir. 1990), this Court held that Executive Branch decisions about what items should be subject to export controls under the EAR present "political questions" that are not subject to judicial

review. See 914 F.2d at 1222-23. The Court explained, inter alia, that the criteria governing the imposition of export controls under the EAR, including the effect of the controls on "the foreign policy or national security interests of the United States," are "quintessentially matters of policy entrusted by the Constitution to the Congress and the President, for which there are no meaningful standards of judicial review." 914 F.2d at 1223; see also United States v. Martinez, 904 F.2d 601, 602-603 (11th Cir. 1990).

We do not suggest that decisions like Waterman and Mandel preclude Bernstein from pursuing his First Amendment claim altogether. However, they make clear the degree of judicial restraint that must accompany the resolution of that claim. Judgments about the effect of export controls on our national security and foreign policy interests are "delicate, complex, and involve large elements of prophecy," and they are ones for which "the Judiciary has neither aptitude, facilities nor responsibility." Waterman, 333 U.S. at 111. The fact that they are presented in the context of a First Amendment claim does not make them any more amenable to judicial resolution.

With these considerations in mind, we turn first to Bernstein's argument that the EAR's exception for printed materials (see 15 C.F.R. 734.3(b)(2) and Note

following 15 C.F.R. 734.3(b)(3)) renders the export controls on encryption software a nullity. Citing Florida Star v. B.J.F., 491 U.S. 524 (1989), Bernstein argues (at 46) that "when the information subject to regulation is [already] publicly available" (emphasis added), continued efforts to suppress the information are unavailing. But the EAR's export controls are not aimed at suppressing the public dissemination of information at all, and hence the fact that people may disseminate cryptographic information abroad by exporting books and other publications containing printed source code is immaterial.

Alternatively, Bernstein argues (at 47) that the printed-material exception defeats the government's efforts to control the use of strong encryption products abroad because anyone who possesses a book or journal containing encryption source code can, in principle, produce functioning encryption software by typing or "scanning" the printed material into a computer. However, not only is the process of turning printed source code into functioning software cumbersome, but it offers no assurance to the user that he will wind up with software that actually maintains the secrecy of his communications. Even the most minute error in this process, such as mistyping or mis-scanning a single character or number in source code that is tens of thousands of characters long, can result in an encryption program that does not work

at all -- or, worse yet (from the user's perspective), a program that runs but does not provide the expected encryption "strength."[7] A computer-ready, error-free diskette or computer file containing encryption software provides a substantially easier and more reliable basis for performing encryption on a computer. It defies common sense to suggest, as Bernstein does, that foreign demand for functioning encryption software is fully satisfied by the export of cryptographic books and magazines, and that the actual use of strong encryption abroad would not materially increase if controls on the export of computer-ready encryption software were abandoned.[8]

---

[7] Encryption programs often contain so-called "magic numbers" -- long, seemingly arbitrary numbers that are used by the programs' encryption algorithms. See, e.g., Bruce Schneier, Applied Cryptography 423 (2d ed. 1996). Inadvertently changing a "magic number" can compromise the software's encryption capabilities.

[8] Bernstein argues (at 25) that one of the particular activities in which he wishes to engage, the posting of encryption software on unrestricted Internet sites, has no national security implications. However, the Congressional testimony on which he relies does not support that conclusion. The point of the quoted testimony is not that Internet distribution of encryption software is irrelevant to the government's national security and foreign policy concerns, but rather that the existing availability of encryption software on the Internet does not itself eliminate the need for export controls. It bears repeating, moreover, that the export controls invalidated by the district court encompass far more than Internet distribution. "'The First Amendment does not bar application of a neutral regulation that incidentally burdens speech merely because a party contends that allowing an exception in [a] particular case will not threaten important governmental interests.'" FTC v. Superior Court Trial Lawyers Ass'n, 493 U.S. 411, 430 (1990)); Ward, 491 U.S. at 801 (validity of regulation under (continued...)

Bernstein's argument (at 48) about the availability of encryption software abroad is similarly misconceived. Here again, Bernstein fails to distinguish between theoretical availability and actual use. Thus far, the availability of encryption software abroad has not translated into widespread use. See, e.g., AER 374 (Congressional testimony of Deputy Director of NSA) ("The fact of the matter is that encryption is widely available * * * but is not widely used") (emphasis in original).[9] Allowing the unrestricted export of encryption software from this country, without regard to its strength and attractiveness to foreign users, can only be expected to

---

[8](...continued)
intermediate First Amendment scrutiny "depends on the relation it bears to the overall problem the government seeks to correct, not on the extent to which it furthers the government's interests in an individual case").

[9] The anecdotal materials cited by the industry amici (Maynard Ferguson et al.) fall far short of supporting their claim (at 23) that strong stand-alone encryption products "are commonly used by the entities in whose communications the U.S. intelligence community is interested" (emphasis added). The National Research Council report cited by the amici states only that "some foreign targets of interest to the U.S. government" use unbreakable encryption. National Research Council, Cryptography's Role in Securing the Information Society 129 (1996) (emphasis added).

result in greater use of such software abroad and correspondingly greater harm to this country's vital signals intelligence capabilities.[10]

It is possible, of course, that foreign availability may affect the potential national security consequences of particular exports to particular destinations and users. But the EAR's export controls already recognize that possibility and permit the Department of Commerce to take it into account in licensing decisions. As noted in our opening brief, the President's Executive Order gives the Department the discretion to consider the significance of foreign availability on a case-by-case basis. See Executive Order 13206, 61 Fed. Reg. 58767 (Nov. 19, 1996). What Bernstein is urging is a fundamentally different regulatory regime -- one in which the bare availability of encryption software abroad automatically results in the uncontrolled export of all domestic encryption software, regardless of its capabilities, regardless of the country, organization, or individuals to whom it is being exported, and regardless of the uses to which they will put it. Nothing in the Constitution requires such a result.

---

[10] We note that many other countries have laws that control the export of encryption products. See Department of Commerce & National Security Agency, A Study of the International Market for Computer Software with Encryption II-9 to II-32 (1996). As a result, there is not an undifferentiated "overseas" market in which encryption software circulates freely.

E. Bernstein suggests (at 49-50) that the EAR's export controls are constitutionally deficient, even under the standards applicable to content neutral regulations, because they restrict "too much speech." However, as explained in our opening brief, a content neutral regulation is sufficiently narrowly tailored as long as the government's interests """would be achieved less effectively absent the regulation."'" Turner, 512 U.S. at 662 (quoting Ward, 491 U.S. at 799). That is certainly true here.

Moreover, as discussed above and in our opening brief, the EAR leaves open ample alternative avenues for the communication of information and ideas about cryptography, including (but not limited to) the unrestricted export of cryptographic books and other printed publications. Bernstein invokes Reno v. ACLU, 117 S. Ct. 2329 (1997), to argue (at 35-36) that the EAR's incidental restrictions on the use of the Internet cannot be justified by the availability of other communications media like books and magazines. But Reno involved a quintessential example of a content-based law, the Communications Decency Act (CDA), and the Supreme Court dismissed the relevance of alternative media in Reno precisely "because the CDA regulates speech on the basis of its content." 117 S. Ct. at 2348 (emphasis added). In contrast, when the regulations in question are content neutral, as here, the Supreme

Court has made clear that the availability of "alternative channels for communication" is highly relevant. Ward, 114 S. Ct. at 791.

F. Finally, Bernstein argues (at 36-39) that the EAR's export controls are unconstitutional because they "restrict the ability to encrypt speech." This argument, unlike the other First Amendment claims that we have thus far addressed, focuses on the speech that is being encrypted, rather than on the "speech" supposedly embodied in encryption source code itself. Bernstein, joined in this regard by several of the amici, asserts that Americans have a First Amendment right to maintain the confidentiality of their communications and that the government may not restrict that right without a compelling showing of need.

Whether or not this First Amendment theory has any merit in the abstract -- a matter on which we express no view -- it simply has no relevance to the regulatory scheme before this Court. The EAR is not designed to limit the confidentiality of communications between American citizens, and it does not prohibit the domestic use of any encryption software or hardware. This case thus does not present any question about the scope of the government's constitutional power to restrict the domestic use of encryption. What is at issue here is a very different matter -- the export of encryption software for use by foreigners abroad. Assuming arguendo that the First

Amendment protects "individual privacy in communications" (Bernstein Brief 36), it hardly follows that foreigners have a First Amendment right to conceal their communications from this country's foreign intelligence-gathering operations, or that persons in this country are entitled to assist them in acquiring products that will allow them to do so.

IV. The District Court's Declaratory And Injunctive Relief Is Too Broad

A. Read literally, the district court' declaratory judgment and injunction cover encryption object code as well as encryption source code. As we explained in our opening brief, however, the district court's prior restraint theory simply does not apply to object code, because "humans cannot read object code" (Sega Enterprises, Ltd. v. Accolade, Inc., 977 F.2d 1510, 1525 (9th Cir. 1993) (emphasis in original)), and the export of object code therefore does not lend itself in any way to use as a means of conveying information and ideas. See Government Brief 45-46.

Bernstein does not claim that programmers (or anyone else) exchange object code to communicate cryptographic ideas with each other, nor does he claim that he himself wishes to do so. Instead, he argues (at 51) that object code should be treated like source code for First Amendment purposes "[b]y analogy" to the Copyright Act. But the status of object code under the Copyright Act is purely a statutory question,

not a constitutional one, and the resolution of that statutory question does not turn on whether object code conveys information to human beings. See Apple Computer, Inc. v. Formula International Inc., 725 F.2d 521, 524-25 (9th Cir. 1984); Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240, 1248 (3d Cir.), cert. dismissed, 464 U.S. 1033 (1984). In contrast, the threshold issue under the First Amendment is "whether `[a]n intent to convey a particularized message [is] present, and [whether] the likelihood [is] great that the message would be understood by those who view[] it.'" Texas v. Johnson, 491 U.S. 397, 404 (1989) (emphasis added) (quoting Spence v. Washington, 418 U.S. 405, 410-11 (1974)); Clark, 468 U.S. at 294. Object code does not even arguably clear this hurdle.

Bernstein also asserts (at 52) that the government is improperly asking this Court to "excise 'object code' from the [EAR's] regulatory control of 'encryption software.'" This argument gets the matter exactly backward. It is the district court that has "excised" encryption object code from the EAR. The government is asking this Court to put it back. "Encryption object code" and "encryption source code" are separately defined by the EAR (see 15 C.F.R. Part 772); no principle of constitutional

adjudication or statutory construction requires discarding export controls over the one because of claimed constitutional infirmities involving the other.[11]

B. The district court's declaratory judgment and injunction also purport to cover encryption "devices" -- a term that is undefined in the EAR, but one that the district court may have used as a synonym for encryption "commodities" (that is, hardware). See Government Brief 46-47. Bernstein asserts that the court did not use "devices" to refer to encryption commodities. But other language in the district court's judgment explicitly covers encryption software and encryption technology. (see ER 574), and encryption commodities are the only other kind of encryption items subject to the EAR. See 15 C.F.R. Part 772 ("encryption items" means "encryption commodities, software, and technology"). Either "devices" refers to commodities, in which case it is wrong, or it does not, in which case it has no regulatory meaning at all. It should be stricken in either case.

C. Finally, the district court purported to strike down the EAR's provisions regarding encryption technology, including 15 C.F.R. 744.9, without deciding

---

[11] If Bernstein is suggesting that the controls on encryption source code are not severable from the other encryption export controls, he is simply wrong. See Alaska Airlines, Inc. v. Brock, 480 U.S. 678, 684 (1987) (summarizing severability standards).

whether those provisions are constitutional. We showed in our opening brief (at 48-50) that Bernstein lacks standing to challenge the constitutionality of the encryption technology provisions because they do not restrict any of his academic activities. We further showed (at 50-52) that, even if Bernstein had standing, 15 C.F.R. 744.9 is plainly constitutional in light of this Court's decision in Edler, supra.

Bernstein makes no response to our standing argument, but he takes issue (at 53-54) with our reliance on Edler. He first argues (at 53) that 15 C.F.R. 744.9 "foster[s] self-censorship" and that Edler did not address this concern. But Section 744.9 provides explicitly that "mere teaching or discussion of information about cryptography, including * * * in an academic setting," is not sufficient to trigger the regulation's licensing requirement. In light of this language, we fail to see how Section 744.9 even arguably "fosters self-censorship" in the academic setting.[12]

Bernstein also suggests (at 53-54) that Edler's First Amendment reasoning is confined to technical assistance involving military products, while Section 744.9 (and the EAR more generally) apply to "dual use" items that have civilian as well as

---

[12] Bernstein's assertion (at 54) that Section 744.9 "clearly applies to purely academic 'technical assistance'" likewise fails to take account of this language.

military or strategic uses.[13] But Edler rests on a more general principle: that when the government legitimately controls the export of products whose use abroad could compromise our national security and foreign policy interests, the government may also regulate technical assistance that would circumvent such controls by intentionally aiding the foreign production of the controlled products. That principle does not depend on whether the controlled product is characterized as "military" or "non-military," and it applies with equal force here.

[13] Bernstein appears to suggest (at 54) that the EAR's export controls are limited to items that have only non-military applications. That is simply incorrect. See 15 C.F.R. 730.3 (defining "dual use" items).

CONCLUSION

For the foregoing reasons, the judgment of the district court should be reversed.

Respectfully submitted,

FRANK W. HUNGER
Assistant Attorney General

MICHAEL J. YAMAGUCHI
United States Attorney

STEPHEN W. PRESTON
Deputy Assistant Attorney General

DOUGLAS N. LETTER
SCOTT R. McINTOSH
Attorneys, Appellate Staff
Civil Division, Room 9550
Department of Justice
601 D Street, N.W.
Washington, D.C. 20530-0001