Govt. Reply to Opposition to Motion for Stay, Sept. 22, 1997 in Bernstein v. Commerce

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

If you want to view or print this document in pieces, here are the first ten pages and remaining pages . You can also download the individual image files, named "page01.gif", "page02.gif", etc. (1 through 14).

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

DANIEL J. BERNSTEIN, Plaintiff-Appellee, v. DEPARTMENT OF COMMERCE et al., Defendants-Appellants.	No. 97-16686

APPELLANTS' REPLY TO APPELLEE'S OPPOSITION TO EMERGENCY MOTION FOR STAY PENDING APPEAL

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
Room 3127, Civil Division
Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

INTRODUCTION

The issue now before this Court is not, as Professor Bernstein repeatedly suggests, whether he may engage in academic discourse relating to cryptography during the pendency of this appeal. He may. As explained by William Reinsch, the Department of Commerce's Under Secretary for Export Administration, "the academic activities that Dr. Bernstein has stated he wishes to undertake, such as the publication of his research on cryptography, public discussion thereof (including overseas), [and] teaching students (including foreign students in the United States[,] are not regulated — nor has the Commerce Department at any time sought to regulate these activities * * * ." Reinsch Dec. ¶ 10 (emphasis added). The stay sought by the Department is not intended to prevent, and will not prevent, these activities.

The issue before this Court is, instead, whether Bernstein should be permitted to engage in the unlimited export of functioning software designed to maintain the secrecy of electronic communications — the type of software whose unrestricted use by foreign intelligence targets has been determined by the President of the United States to pose a genuine risk to our national security, foreign policy, and law enforcement interests. The answer to that question is plainly "no." The decision below rests on an unprecedented and highly dubious First Amendment ruling — a ruling that restrictions on the export of encryption software, which are not directed at the free flow of information regarding cryptography and which have been in effect in substantially the same form for decades, are a facially unconstitutional prior restraint on speech. Bernstein has relatively little to say in defense of this novel prior restraint ruling, and what he does say is misconceived. At the

same time, Bernstein does not dispute that the district court's injunction permits him to export his encryption software, in its current form or modified forms, to any persons abroad, by any means and in any volume, for any purpose whatsoever. The risks posed by this kind of unrestricted export are obvious, and nothing in Bernstein's opposition diminishes those risks. In these circumstances, simple prudence counsels that this Court maintain the status quo while expediting this appeal, rather than allowing Bernstein to engage in the immediate and irreversible export of encryption software that the President has directed the Department of Commerce to regulate under the EAR.

I. The District Court's First Amendment Ruling Is Likely To Be Reversed

A. The judgment below holds that the provisions of the EAR relating to the export of encryption software are facially invalid under the prior restraint doctrine. As explained in our stay motion, this prior restraint ruling is not only "novel," as the district court itself acknowledged, but very much at odds with established First Amendment principles. This is not a case, like the Pentagon Papers case, in which the government is seeking to restrain speech in order to impede the free flow of information and ideas. As the President's Executive Order and the terms of the EAR itself make abundantly clear, the regulatory scheme invalidated by the district court is aimed at the capacity of encryption software (and other encryption products) to insulate foreign intelligence targets from this country's electronic intelligence-gathering efforts, not at the information about cryptography that particular encryption source code might be claimed to reflect or convey. And because the

EAR is a "law[] of general application that [is] not aimed at conduct commonly associated with expression" (City of Lakewood v. Plain Dealer Publishing Co., 486 U.S. 750, 760-61 (1988)), it does not have a "close enough nexus to expression, or to conduct commonly associated with expression" (id. at 759), to be subject to a facial challenge on prior restraint grounds. See Motion 14-19.

In response to our prior restraint analysis, Bernstein points to a number of decisions of this Court that have subjected "licensing schemes directed at expression" (Opp. 17) to facial invalidation on prior restraint grounds. In each of these cases, however, the licensing scheme at issue was targeted at activities that are undertaken exclusively for expressive purposes, such as posting commercial signs, distributing handbills, soliciting charitable contributions and sales, or speaking and demonstrating in a public park.[1] As a result, the licensing schemes understandably were found to have a sufficient "nexus to expression, or to conduct commonly associated with expression" (Lakewood, 486 U.S. at 759), to pose a substantial risk of censorship and therefore warrant facial invalidation. The regulatory scheme at issue here is fundamentally different, for it encompasses a vast array of items and activities that are not even arguably expressive, and even the specific activity invoked by

---

[1] See Desert Outdoor Advertising, Inc. v. City of Moreno Valley, 103 F.3d 814, 816-17 (9th Cir. 1996) (posting commercial signs); Grossman v. City of Portland, 33 F.3d 1200, 1201 (9th Cir. 1994) (speaking and demonstrating in public park); Gerritson v. City of Los Angeles, 994 F.2d 570, 573-74 (distributing handbills); Gaudiya Vaishnava Society v. City and County of San Francisco, 952 F.2d 1059, 1062 (9th Cir. 1990) ("charitable sales solicitation"); Carreras v. City of Anaheim, 768 F.2d 1039, 1041-42, 1047-50) (soliciting charitable donations); Rosen v. Port of Portland, 641 F.2d 1244-45 & n.2 (soliciting donations and speaking in airports).

Bernstein — the distribution of software in source code form — is routinely undertaken for the wholly non-expressive purpose of enabling persons to control the operation of computers. See Motion 15-16. Nothing in this Court's decisions cited by Bernstein supports the facial invalidation of such a regulatory scheme.[2]

B. Bernstein argues at length that encryption source code is capable of being understood by computer scientists and programmers (Opp. 15-17). But it simply does not follow from this proposition, as Bernstein suggests, that government regulations restricting the export of encryption source code are therefore subject to strict scrutiny under the First Amendment.

As Bernstein himself concedes, even if source code theoretically can be understood by persons trained in computer programming, it nonetheless also is "'a way of getting a computer to perform operations'" (Opp. 16). This capability of source code to "get[] a computer to perform operations" exists even when the person using the source code is neither able to understand it nor interested in doing so. It is this capability that leads the EAR to restrict the export of encryption source code, just as it restricts the export of other items

---

[2] Bernstein's reliance on such cases as Secretary of State v. Joseph H. Munson Co., 467 U.S. 947 (1984), and Schaumberg v. Citizens for a Better Environment, 444 U.S. 620 (1980), is misplaced for similar reasons. Munson and Schaumberg involved government licensing of charitable solicitation, an activity that the Court found to be "characteristically intertwined" with the communication of "informative and perhaps persuasive speech" (Schaumberg, 444 U.S. at 632). The Supreme Court determined specifically that "[h]ere there is no core of easily identifiable and constitutionally proscribable conduct that the statute prohibits" (Munson, 467 U.S. at 965-66). In contrast, the EAR in general, and even the EAR's encryption provisions in particular, cover a wide range of conduct that is not even arguably protected by the First Amendment.

(whether software or hardware) that have encryption capabilities. Because the EAR's export restrictions are not directed at suppressing the purported informational value of encryption source code, but rather at the capability of encryption software to turn computers and other programmable electronic devices into encryption machines, they are content-neutral and hence are subject to the less demanding First Amendment standards of United States v. O'Brien, 391 U.S. 367 (1968), not the strict scrutiny urged by Bernstein and employed by the district court. Motion 9; see Karn v. U.S. Department of State, 925 F. Supp. 1, 9-11 (D.D.C. 1996) (holding similar restrictions on encryption software exports to be content-neutral and therefore subject to O'Brien review), remanded on other grounds, 107 F.3d 923 (D.C. Cir. 1997).[3]

Bernstein asserts that the EAR is not content-neutral, for purposes of O'Brien, because it allegedly singles out software "on the subject of cryptography" for special restrictions (Opp. 14). But the challenged provisions of the EAR are not directed at "the subject of cryptography"; they are directed at items that function to encrypt data, whether the items be software products or hardware devices. And as explained in the stay motion, to the extent that the EAR treats encryption software differently from other software, it does so precisely because the government is not concerned with the potential informational content of

[3] The applicability of O'Brien here depends not on the often-elusive distinction between "speech" and "conduct," but rather on whether the object of the government's regulation is unrelated to the suppression of free expression. See, e.g., Blount v. SEC, 61 F.3d 938, 942 (D.C. Cir. 1995), cert. denied, 116 S. Ct. 1351 (1996); Home Box Office, Inc. v. FCC, 567 F.2d 9, 47-48 (D.C. Cir.) (per curiam), cert. denied, 434 U.S. 829 (1977).

encryption software, but rather with its non-expressive capability to make computers encrypt data. See Motion 19.

As our reliance on O'Brien should make clear, the government is not contending that "it may dispense with constitutional protections" altogether (Opp. 19) when it regulates the export of encryption source code. Rather, we are contending that the EAR's restrictions on the export of encryption software pass constitutional muster under O'Brien, and the district court erred in resorting to the prior restraint doctrine to invalidate the regulations.

C. Bernstein asserts that the EAR's restrictions on the export of encryption software (and, presumably, encryption hardware as well) rest on the premise that "the keeping of messages secret is inherently dangerous" (Opp. 4). However, the provisions in question actually rest on a different proposition: the proposition that this country and its citizens are at risk from the activities of hostile nations, organizations, and individuals abroad, and that the risk is increased by the ability of foreign intelligence targets to conceal information about their activities from American intelligence-gathering efforts. That proposition should be uncontroversial, and it certainly is not constitutionally suspect.[4]

Bernstein argues that if the government can require a license for the export of encryption software, it could likewise require a license for typewriters or fax machines in order to prevent their use to convey "subversive" or "dangerous" ideas (Opp. 20-21). This

[4] In this regard, it should be noted that the EAR is not designed to limit the confidentiality of communications between American citizens and 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 power to restrict the domestic use of encryption.

argument is, to put it bluntly, preposterous. In Bernstein's imaginary examples, licensing regulations are imposed for the purpose of preventing the dissemination of constitutionally protected speech. Here, in contrast, the government does not license the export of encryption items in order to prevent speech, constitutionally protected or otherwise. The goal is not to prevent foreign intelligence targets from communicating with each other, but simply to protect this country's ability to monitor their communications. Thus, even if one indulges in the assumption that speech by foreign intelligence targets is itself constitutionally protected, the EAR — unlike Bernstein's hypothetical licensing schemes — is not a constitutionally suspect attempt to deter that speech.

II. The Balance of Harms and the Public Interest Strongly Favor a Full Stay Pending Appeal

A. Bernstein accuses the government of relying on "bare allegations" and "speculative assertions" of injury to national security (Opp. 7). But it is not speculation that Bernstein's software is designed specifically to enable computers to produce encrypted electronic communications. See Joint Statement of Undisputed Facts ¶ 11 (Sept. 20, 1996). Nor is it speculation that the use by foreign intelligence targets of products that produce data confidentiality compromises the intelligence-gathering capabilities of the United States and thereby "can jeopardize our foreign policy and national security interests" and "threaten the safety of U.S. citizens here and abroad * * * ." 32 Weekly Comp. Pres. Doc. 2397 (Nov. 15, 1996) (Presidential memorandum); Crowell Dec. ¶ 4. To be sure, we do not know to whom Bernstein will export his software, how he will export it, or what versions of the software

he will export. But these matters are unavoidably "speculative," because they are exclusively within the control of Bernstein himself. Indeed, that is a large part of the immediate problem: the district court's injunction and partial stay place no restrictions on Bernstein in any of these regards.

Bernstein points to the Pentagon Papers case (Opp. 8-10) as proof that the government has made an inadequate showing of irreparable injury to support a stay here. As explained in our stay motion, however, the Pentagon Papers case is wholly inapposite, for the government there was seeking to enjoin the publication of the Pentagon Papers precisely in order to prevent the free flow of information to the public. Here, in contrast, the EAR manifestly is not intended to prevent the free flow of information about cryptography, nor does it have that effect — either with respect to Bernstein or more generally. See, e.g., Joint Statement of Undisputed Facts ¶ 9 (Sept. 20, 1996) ("Articles and papers containing and discussing cryptographic algorithms, source code, and theories have been published in scientific journals for many years for peer review and evaluation"). Where the government seeks to impose a prior restraint on the publication of information on a subject of public debate, it is unsurprising that the courts have demanded an exceptionally strong showing of irreparable harm in the absence of the restraint. But where, as here, the regulatory scheme at issue is not directed at the suppression of speech, and where it leaves open ample alternative avenues for disseminating the "information" that the plaintiff assertedly wishes to convey, neither the Pentagon Papers case nor any other case cited by Bernstein suggests

that a comparably demanding showing is required.[5]

B. Bernstein argues that the national security is unlikely to be jeopardized by the distribution of his encryption software over the Internet. However, the fact that the EAR specifically includes electronic distribution of encryption source code and object code (see 15 U.S.C. § 734.2(b)(9)) reflects the government's considered judgment that electronic distribution, if left unrestricted, would create a risk to the national security and foreign policy concerns underlying the EAR. The quoted Congressional testimony of Vice Admiral McConnell and Deputy Director Crowell (Opp. 8) is not to the contrary. The point of their testimony was 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.

Moreover, Bernstein's arguments about Internet distribution fail to come to terms with the actual scope of the district court's injunction. The injunction does not confine Bernstein to exporting his encryption software via the Internet; instead, it permits him to export his software in any manner, including direct export on conventional computer media like

---

[5] Bernstein cites Wildmon v. Berwick Universal Pictures, 983 F.2d 21 (5th Cir. 1992), for the proposition that the government must make a "compelling showing"of need in order to obtain a stay here (Opp. 7). Wildmon, however, did not involve the government at all, but rather concerned a "private contractual matter" between two private parties (983 F.2d at 24). Moreover, the contract underlying the dispute in Wildmon provided for liquidated damages rather than injunctive relief, leading the Court of Appeals to hold that "injunctive relief is virtually waived" (ibid.). Needless to say, there is nothing remotely comparable in this case.

diskettes, and he may do so for commercial as well as non-commercial purposes. Moreover, the injunction and partial stay are not limited to the specific version of Bernstein's encryption software that underlies this litigation (Snuffle 5.0), but rather encompass any and all updated versions of the software as well, including not only versions that Bernstein "has made" in the past (Opp. 10) but those that he may make in the future. As a consequence, Bernstein is free to export even more powerful and useful versions of his software, no matter how effective and desirable they might prove for foreign intelligence targets. Thus, even if Bernstein were correct that the distribution of Snuffle 5.0 over the Internet would not pose a threat to the national security by itself (which we do not concede), that would hardly eliminate the need for a stay of the district court's injunction, which permits the export of any version of Bernstein's software by any means.[6]

C. Bernstein argues (Opp. 11) that the district court's injunction does not create a risk of irreparable injury for the government because, while the EAR generally prohibits the unlicensed export of encryption software, it contains an exception for the export of encryption source code in printed form (e.g., books and magazines). See 15 C.F.R. 734.3(b)(3) Note. However, the government obviously would not have adopted this exception for printed materials if it expected the exception to defeat the goals of the EAR. The government permits the export of printed materials containing encryption source code

[6] Bernstein states that even if he is allowed to export his software, under the terms of the district court's partial stay, "[n]o other person can republish Professor Bernstein's source code" (Opp. 10). To the contrary, after Bernstein exports his source code, anyone overseas can redistribute it electronically.

because the process of transforming printed source code into the error-free electronic form required by computers has thus far been too cumbersome for printed source code to contribute materially to the use of encryption software abroad[7]. In contrast, the injunction at issue in this case permits Bernstein to export his encryption source code in computer-ready form through any electronic medium, including not only the Internet but also conventional computer media like diskettes. As a result, the injunction creates far greater risks that Bernstein's encryption software will actually be put to use abroad.[8]

D. Finally, Bernstein argues that export of his encryption software poses no risk because other encryption programs are available overseas. But the President has expressly determined that "the export of encryption products * * * could harm national security and foreign policy interests even where comparable products are or appear to be available from sources outside the United States * * *." Executive Order 13026, 61 Fed. Reg. 58767 (Nov. 19, 1996) (emphasis added). The bare fact that other encryption software is available abroad says nothing about how widespread the use of other encryption programs may be, nor does it demonstrate that they are as effective as current or future versions of Bernstein's software.

---

[7] The printed-material exception underscores the fact that the government's object is not to prevent the free flow of information about cryptography. As a result, the fact that "cryptographic information is freely available to foreign entities" (Opp. 11) is simply immaterial to the government's legitimate regulatory concerns.

[8] Interestingly, while Bernstein relies on the EAR's printed-material exception to contest the government's showing of irreparable harm, he makes no mention of it when discussing the impact of the EAR on his own academic activities. The existence of the printed-material exception means that Bernstein is free to send his source code in printed form to his academic colleagues abroad for their comments and suggestions.

In our stay motion, we noted that a version of Bernstein's own program had been posted, apparently in violation of federal export laws, on several publicly accessible computers overseas (Motion 21). Bernstein's opposition indicates that the version of Bernstein's program currently available abroad is an earlier version, not the current version (Opp. 15 n.12). As a result, the risks posed by the unrestricted export of Bernstein's software are even greater than we understood them to be at the time that the stay motion was filed.

E. Bernstein asserts that a full stay would subject him to irreparable injury because the EAR "preclude[s] [him] from engaging in traditional academic dialogue in his chosen field" and subjects him to the risk of prosecution "for discussing the science of cryptography" (Opp. 2-3). But the EAR does nothing of the kind. As explained above, the EAR simply does not prohibit "traditional academic dialogue" regarding cryptography, nor does it expose anyone to prosecution for "discussing the science of cryptography." See pp. 1, 8 supra. By the same token, the EAR does not prohibit Bernstein from "publish[ing] any of his other ideas in the field or comment[ing] upon the ideas of others on the Internet" (Opp. 10). To repeat, what is at stake here is Bernstein's ability to engage in the unrestricted export of functional encryption software, not his right to engage in academic discussions about cryptography. As we suggested in our stay motion, the appropriate balance between Bernstein's interests and those of the United States is best served by granting a stay and expediting the appeal, not by throwing open the door to the unlimited export of Bernstein's encryption software for the duration of the appeal.

CONCLUSION

For the foregoing reasons and the reasons set forth in the stay motion, this Court should issue a full stay of the district court injunction pending expedited appeal.[9]

Respectfully submitted,

FRANK W. HUNGER
Assistant Attorney General

MICHAEL J. YAMAGUCHI
United States Attorney

STEPHEN W. PRESTON
Deputy Assistant Attorney General

Douglas N. Letter
DOUGLAS N. LETTER

SCOTT R. McINTOSH

Attorneys, Appellate Staff
Room 3127, Civil Division
Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530
(202) 514-4052

[9] As the Court is aware, Bernstein and the Department of Commerce have executed a joint stipulation under which Bernstein has voluntarily committed himself not to export his encryption program until 5:00 p.m. on Tuesday, September 23. If this Court has not acted on the Department's underlying stay application by that time, the Department renews its request for an immediate temporary stay pending resolution of the underlying stay request.