Case Name:
BERNSTEIN V USDOJ

Case Number: 97-16686

Date Filed: 05/06/99

FOR PUBLICATION

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

DANIEL J. BERNSTEIN,
Plaintiff-Appellee,

v.

UNITED STATES DEPARTMENT OF JUSTICE; UNITED STATES DEPARTMENT OF COMMERCE; DEPARTMENT OF STATE; UNITED STATES DEPARTMENT OF DEFENSE; UNITED STATES ARMS CONTROL AND DISARMANENT AGENCY; NATIONAL SECURITY AGENCY; UNITED STATES DEPARTMENT OF ENERGY; CENTRAL INTELLIGENCE AGENCY; MADELINE E. ALBRIGHT, United States Secretary of State; WILLIAM M. DALEY, United States Secretary of Commerce; WILLIAM COHEN, United States Secretary of Defense; KENNETH A. MINIHAN, Director, United States National Security Agency; JOHN B. HOLUM, Director, United States Arms Control and Disarmanent Agency; WILLIAM G. ROBINSON; GARY M. ONCALE; AMBASSADOR MICHAEL NEWLIN; CHARLES RAY; MARK KORO; GREG STARK; DOES 1-100,
Defendants-Appellants.

No. 97-16686
D.C. No.
CV-97-00582
MHP
OPINION

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

Marilyn Hall Patel, District Judge, Presiding

4215

Argued and Submitted
December 8, 1997--San Francisco, California

Filed May 6, 1999

Before: Myron H. Bright,* Betty B. Fletcher, and Thomas G. Nelson, Circuit Judges.

Opinion by Judge B. Fletcher; Concurrence by Judge Bright; Dissent by Judge T.G. Nelson

4251

COUNSEL

Scott R. McIntosh (argued), Douglas N. Letter, United States Department of Justice, Washington, D.C., for the defendants-appellants.

Cindy A. Cohn (argued), McGlashan & Sarrail, San Mateo, California, and Lee Tien, Berkeley, California, for the plaintiff-appellee.

Ivan K. Fong, Covington & Burling, Washington, D.C., for amicus curiae Electronic Privacy Information Center; American Civil Liberties Union; American Civil Liberties Union of Northern California; Center For Democracy and Technology; Computer Professionals for Social Responsibility; Economic Strategy Institute; Free Congress Research and Education Foundation; Human Rights Watch; Independence Institute; International Information System Security Certification Consortium; Internet Mail Consortium; Internet Society; National Association of Manufacturers; Privacy International; U.S. Public Policy Committee of the Association for Computing; Dr. Whitfield Diffie; Dr. Peter Neumann; and Dr. Ronald Rivest.

Garrett Epps, University of Oregon School of Law, Eugene, Oregon, for amicus curiae Silicon Valley Software Industry Coalition; Professor Keith Aoki; Professor Margreth Barrett; Professor James Boyle; Professor Garrett Epps; Professor Peter Jaszi; Professor David Lange; and Professor Eugene Volokh.

Brian Conboy, Wilkie Farr & Gallagher, Washington, D.C., for amicus curiae Maynard Anderson; D. James Bidzos;

4221

National Computer Security Association; Mark Rasch; RSA Data Security, Inc.; Dr. Eugene Spafford; and Dr. Ross Stapleton-Gray.

J. Joshua Wheeler, Charlottesville, Virginia, for amicus curiae Thomas Jefferson Center for the Protection of Free Expression.

Richard D. Marks, Vinson & Elkins, Washington, D.C., for amicus curiae Association for the Advancement of Science.

OPINION

B. FLETCHER, Circuit Judge:

The government defendants appeal the grant of summary judgment to the plaintiff, Professor Daniel J. Bernstein ("Bernstein"), enjoining the enforcement of certain Export Administration Regulations ("EAR") that limit Bernstein's ability to distribute encryption software. We find that the EAR regulations (1) operate as a prepublication licensing scheme that burdens scientific expression, (2) vest boundless discretion in government officials, and (3) lack adequate procedural safeguards. Consequently, we hold that the challenged regulations constitute a prior restraint on speech that offends the First Amendment. Although we employ a somewhat narrower rationale than did the district court, its judgment is accordingly affirmed.

BACKGROUND

A. Facts and Procedural History

Bernstein is currently a professor in the Department of Mathematics, Statistics, and Computer Science at the University of Illinois at Chicago. As a doctoral candidate at the Uni-

4222

versity of California, Berkeley, he developed an encryption method -- "a zero-delay private-key stream encryptor based upon a one-way hash function"1 -- that he dubbed "Snuffle." Bernstein described his method in two ways: in a paper containing analysis and mathematical equations (the "Paper") and in two computer programs written in "C," a high-level computer programming language ("Source Code"). Bernstein later wrote a set of instructions in English (the "Instructions") explaining how to program a computer to encrypt and decrypt data utilizing a one-way hash function, essentially translating verbatim his Source Code into prose form.

Seeking to present his work on Snuffle within the academic and scientific communities, Bernstein asked the State Department whether he needed a license to publish Snuffle in any of its various forms. The State Department responded that Snuffle was a munition under the International Traffic in Arms Regulations ("ITAR"), and that Bernstein would need a license to "export" the Paper, the Source Code, or the Instructions.2 There followed a protracted and unproductive series of letter communications between Bernstein and the government, wherein Bernstein unsuccessfully attempted to

---

1 The term "hash function" describes a function that transforms an input into a unique output of fixed (and usually smaller) size that is dependent on the input. For some purposes (e.g. error checking, digital signatures), it is desirable that it be impossible to derive the input data given only the hash function's output -- this type of function is known as a "one-way hash function." Hash functions have many uses in cryptography and computer science, and numerous one-way hash functions are widely known. "Zero-delay" means that Snuffle can be used for interactive communications because it encrypts and decrypts on a character-by-character basis -- the users need not complete an entire message before encrypting and sending.

2 In June 1995, after Bernstein initiated this suit, the State Department clarified its earlier determination, explaining that while ITAR did restrict the Source Code and the Instructions, it did not restrict the Paper.

4223

determine the scope and application of the export regulations to Snuffle.3

Bernstein ultimately filed this action, challenging the constitutionality of the ITAR regulations. The district court found that the Source Code was speech protected by the First Amendment, see Bernstein v. Department of State , 922 F. Supp. 1426 (N.D. Cal. 1996) ("Bernstein I"), and subsequently granted summary judgment to Bernstein on his First Amendment claims, holding the challenged ITAR regulations facially invalid as a prior restraint on speech, see Bernstein v. Department of State, 945 F. Supp. 1279 (N.D. Cal. 1996) ("Bernstein II").

In December 1996, President Clinton shifted licensing authority for nonmilitary encryption commodities and technologies from the State Department to the Department of Commerce. See Exec. Order No. 13,026, 61 Fed. Reg. 58,767 (1996). The Department of Commerce then promulgated regulations under the EAR to govern the export of encryption technology, regulations administered by the Bureau of Export Administration ("BXA"). See 61 Fed. Reg. 68,572 (1996) (codified at 15 C.F.R. Pts. 730-74). Bernstein subsequently amended his complaint to add the Department of Commerce

as a defendant, advancing the same constitutional objections as he had against the State Department. The district court, following the rationale of its earlier Bernstein opinions, once again granted summary judgment in favor of Bernstein, finding the new EAR regulations facially invalid as a prior restraint on speech. See Bernstein v. Department of State, 974

---

3 Bernstein notes that his difficulties with the State Department are by no means unique. Declarations provided by Bernstein demonstrate ongoing suppression of academic publication by the State Department under ITAR. See Demberger Decl. (found in violation of ITAR for posting encryption program on the internet); Junger Decl. (stated that ITAR caused him to censor publication of his work for fear of violating the regulations); Zimmerman Decl. (target of a criminal investigation for publishing encryption software on the internet).

F. Supp. 1288 (N.D. Cal. 1997) ("Bernstein III"). The district court enjoined the Commerce Department from future enforcement of the invalidated provisions, an injunction that has been stayed pending this appeal.

B. Overview of Cryptography

Cryptography is the science of secret writing, a science that has roots stretching back hundreds, and perhaps thousands, of years. See generally DAVID KHAN, THE CODEBREAKERS (2d ed. 1996). For much of its history, cryptography has been the jealously guarded province of governments and militaries. In the past twenty years, however, the science has blossomed in the civilian sphere, driven on the one hand by dramatic theoretical innovations within the field, and on the other by the needs of modern communication and information technologies. As a result, cryptography has become a dynamic academic discipline within applied mathematics. It is the cryptographer's primary task to find secure methods to encrypt messages, making them unintelligible to all except the intended recipients:

> Encryption basically involves running a readable message known as "plaintext" through a computer program that translates the message according to an equation or algorithm into unreadable "ciphertext." Decryption is the translation back to plaintext when the message is received by someone with an appropriate "key."

Bernstein III, 974 F. Supp. at 1292. The applications of encryption, however, are not limited to ensuring secrecy; encryption can also be employed to ensure data integrity, authenticate users, and facilitate nonrepudiation (e.g., linking a specific message to a specific sender). See id.

It is, of course, encryption's secrecy applications that concern the government. The interception and deciphering of for-

eign communications has long played an important part in our nation's national security efforts. In the words of a high-ranking State Department official:

> Policies concerning the export control of cryptographic products are based on the fact that the proliferation of such products will make it easier for foreign intelligence targets to deny the United States Government access to information vital to national security interests. Cryptographic products and software have military and intelligence applications. As demonstrated throughout history, encryption has

> been used to conceal foreign military communications, on the battlefield, aboard ships and submarines, or in other military settings. Encryption is also used to conceal other foreign communications that have foreign policy and national security significance for the United States. For example, encryption can be used to conceal communications of terrorists, drug smugglers, or others intent on taking hostile action against U.S. facilities, personnel, or security interests.

Lowell Decl. at 4 (reproduced in Appellant's Excerpts of Record at 97). As increasingly sophisticated and secure encryption methods are developed, the government's interest in halting or slowing the proliferation of such methods has grown keen. The EAR regulations at issue in this appeal evidence this interest.

C. The EAR regulations[4]

The EAR contain specific regulations to control the export of encryption software, expressly including computer source

---

4 Because the district court capably detailed the ITAR and EAR regulatory regimes, see Bernstein III, 974 F. Supp. at 1292–96, we present only an overview of the relevant provisions here.

code. Encryption software is treated differently from other software in a number of significant ways. First, the term "export" is specifically broadened[5] with respect to encryption software to preclude the use of the internet and other global mediums if such publication would allow passive or active access by a foreign national within the United States or anyone outside the United States. 15 C.F.R. § 734.2(b)(9)(B)(ii).[6] Second, the regulations governing the export of nonencryption software provide for several exceptions that are not applicable to encryption software.[7] In addition, although printed materials containing encryption source code are not subject to EAR regulation, the same materials made available on machine-readable media, such as floppy disk or CD-ROM, are covered. 15 C.F.R. § 734.3(b), Note to Paragraphs (b)(2) & (b)(3). The government, moreover, has reserved the right to restrict source code in printed form that may be easily "scanned," thus creating some ambiguity as to whether

---

5 "Export," even as applied to software generally, is defined quite broadly to include any release, including oral exchanges of information and visual inspections, in a foreign country or to a foreign national within the United States. 15 C.F.R. § 734.2(b)(2) & (3).

6 Specifically, 15 C.F.R. § 734.2(b)(9)(B)(ii) provides that "export" includes:

> downloading or causing the downloading of, such software to locations (including electronic bulletin boards, Internet file transfer protocol, and World Wide Web sites) outside the U.S., or making such software available for transfer outside the United States, over wire, cable, radio, electromagnetic, photo-optical, photoelectric or other comparable communications facilities accessible to persons outside the United States, including transfers from electronic bulletin boards, Internet file transfer protocol and World Wide Web sites, unless the person making the software available takes precautions adequate to prevent unauthorized transfer of such code outside the United States.

7 These exceptions allow for export of software that is publicly available, 15 C.F.R. § 734.7(c); results from fundamental research or is educational, 15 C.F.R. §§ 734.3(b)(3), 734.8, 734.9; is already available from foreign sources, 15 C.F.R. § 768.1(b); or contains only a de minimis quantity of domestically-derived content, 15 C.F.R.§ 734.4(b)(2).

printed publications are necessarily exempt from licensing. See 61 Fed. Reg. 68,575 (1996).

If encryption software falls within the ambit of the relevant EAR provisions, the "export" of such software requires a prepublication license. When a prepublication license is requested, the relevant agencies undertake a "case-by-case" analysis to determine if the export is "consistent with U.S. national security and foreign policy interests." 15 C.F.R. S 742.15(b). All applications must be "resolved or referred to the President no later than 90 days" from the date an application is entered into the BXA's electronic license processing system. 15 C.F.R. S 750.4(a). There is no time limit, however, that applies once an application is referred to the President. Although the regulations do provide for an internal administrative appeal procedure, such appeals are governed only by the exhortation that they be completed "within a reasonable time." 15 C.F.R. S 756.2(c)(1). Final administrative decisions are not subject to judicial review. 15 C.F.R. S 756.2(c)(2).

DISCUSSION

I. Prior Restraint

The parties and amici urge a number of theories on us. We limit our attention here, for the most part, to only one: whether the EAR restrictions on the export of encryption software in source code form constitute a prior restraint in violation of the First Amendment. We review de novo the district court's affirmative answer to this question. See Roulette v. Seattle, 97 F.3d 300, 302 (9th Cir. 1996).

[1] It is axiomatic that "prior restraints on speech and publication are the most serious and least tolerable infringement on First Amendment rights." Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 559 (1976). Indeed, the Supreme Court has opined that "it is the chief purpose of the [First Amendment] guaranty to prevent previous restraints upon publication." Near v.

Minnesota, 283 U.S. 697, 713 (1931). Accordingly, "[a]ny prior restraint on expression comes . . . with a `heavy presumption' against its constitutional validity." Organization for a Better Austin v. Keefe, 402 U.S. 415, 419 (1971). At the same time, the Supreme Court has cautioned that"[t]he phrase `prior restraint' is not a self-wielding sword. Nor can it serve as a talismanic test." Kingsley Books, Inc. v. Brown, 354 U.S. 436, 441 (1957). We accordingly turn from"[t]he generalization that prior restraint is particularly obnoxious" to a "more particularistic analysis." Id. at 442.

[2] The Supreme Court has treated licensing schemes that act as prior restraints on speech with suspicion because such restraints run the twin risks of encouraging self-censorship and concealing illegitimate abuses of censorial power. See Lakewood v. Plain Dealer Publishing Co., 486 U.S. 750, 759 (1988). As a result, "even 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." Id. at 764 (emphasis in original). We follow the lead of the Supreme Court and divide the appropriate analysis into two parts. The threshold question is whether Bernstein is entitled to bring a facial challenge against the EAR regulations. See id. at 755. If he is so entitled, we proceed to the second question: whether the regulations constitute an impermissible prior restraint on speech. See id. at 769.

A. Is Bernstein entitled to bring a facial attack?

[3] A licensing regime is always subject to facial challenge8

---

8 In using the term "facial challenge" in the prior restraint context, the Supreme Court has meant two distinct things. First, if entitled to bring a facial challenge, a plaintiff need not apply for a license before challenging the licensing regime. See Lakewood, 380 U.S. at 755–56. This is a question of standing. Second, a litigant challenging an enactment on its face champions the rights of those not before the court and thus may attack the statute "whether or not his conduct could be proscribed by a properly drawn statute." Freedman v. Maryland, 380 U.S. 51, 56 (1965); see also Secretary of State of Md. v. J. H. Munson Co., 467 U.S. 947, 957 (1984); Roulette, 97 F.3d at 303 n.3. This goes to the scope of the constitutional challenge.

4229

as a prior restraint where it "gives a government official or agency substantial power to discriminate based on the content or viewpoint of speech by suppressing disfavored speech or disliked speakers," and has "a close enough nexus to expression, or to conduct commonly associated with expression, to pose a real and substantial threat of . . . censorship risks." Id. at 759.

[4] The EAR regulations at issue plainly satisfy the first requirement -- "the determination of who may speak and who may not is left to the unbridled discretion of a government official." Id. at 763. BXA administrators are empowered to deny licenses whenever export might be inconsistent with "U.S. national security and foreign policy interests." 15 C.F.R. S 742.15(b). No more specific guidance is provided. Obviously, this constraint on official discretion is little better than no constraint at all. See Lakewood, 486 U.S. at 769–70 (a standard requiring that license denial be in the "public interest" is an "illusory" standard that "renders the guarantee against censorship little more than a high-sounding ideal."). The government's assurances that BXA administrators will not, in fact, discriminate on the basis of content are beside the point. See id. at 770 (presumption that official will act in good faith "is the very presumption that the doctrine forbidding unbridled discretion disallows."). After all,"the mere existence of the licensor's unfettered discretion, coupled with the power of prior restraint, intimidates parties into censoring their own speech, even if the discretion and power are never actually abused." Id. at 757.

4230

The more difficult issue arises in relation to the second requirement -- that the challenged regulations exhibit "a close enough nexus to expression." We are called on to determine whether encryption source code is expression for First Amendment purposes.9

We begin by explaining what source code is.10 "Source code," at least as currently understood by computer programmers, refers to the text of a program written in a "high-level" programming language, such as "PASCAL" or "C." The distinguishing feature of source code is that it is meant to be read and understood by humans and that it can be used to express an idea or a method. A computer, in fact, can make no direct use of source code until it has been translated ("compiled") into a "low-level" or "machine" language, resulting in computer-executable "object code." That source code is meant for human eyes and understanding, however, does not mean that an untutored layperson can understand it. Because source code is destined for the maw of an automated, ruthlessly literal translator -- the compiler -- a programmer must

---

9 As an initial matter, we note that the fact that the regulations reach only

"exports" does not reduce the burden on Bernstein's First Amendment rights. It is Bernstein's right to speak, not the rights of foreign listeners to hear, that we are concerned with here. The government does not argue, nor could it, that being cut off from a foreign audience, as distinguished from a domestic one, does not implicate First Amendment concerns. See Bullfrog Films, Inc. v. Wick, 847 F.2d 502, 509 n.9 (9th Cir. 1988). In addition, because the regulations define "export" to include the use of internet fora that may be accessible by foreign nationals, as well as domestic communications with foreign nationals, we think it plain that the regulations potentially limit Bernstein's freedom of speech in a variety of both domestic and foreign contexts. See Reno v. American Civ. Lib. Union, 117 S. Ct. 2329, 2348–49 (1997) (rejecting government argument that restriction of expression on the internet is justified because ample alternative channels of communication exist).

10 In undertaking this task, we are mindful that computer technology, and the lexicon of terms that accompanies it, is changing rapidly. Nevertheless, because the regulations speak in terms of "source code," we premise our discussion on the meaning commonly ascribed to this term by the programming community.

follow stringent grammatical, syntactical, formatting, and punctuation conventions. As a result, only those trained in programming can easily understand source code.11

Also important for our purposes is an understanding of how source code is used in the field of cryptography. Bernstein has submitted numerous declarations from cryptographers and computer programmers explaining that cryptographic ideas and algorithms are conveniently expressed in source code.12

---

11 It must be emphasized, however, that source code is merely text, albeit text that conforms to stringent formatting and punctuation requirements. For example, the following is an excerpt from Bernstein's Snuffle source code:

```
for (;;)
    (
    uch = gtchr();
    if (!(n & 31))
        (
          for (i = 0; i64; i++)
              l [ ctr[i] ] = k[i] + h[n – 64 + i]
          Hash512 (wm, wl, level, 8);
        )
```

As source code goes, Snuffle is quite compact; the entirety of the Snuffle source code occupies fewer than four printed pages.

12 Source code's power to convey algorithmic information is illustrated by the declaration of MIT Professor Harold Abelson:

> The square root of a number X is the number Y such that Y times Y equals X. This is declarative knowledge. It tells us something about square roots. But it doesn't tell us how to find a square root.
>
> In contrast, consider the following ancient algorithm, attributed to Heron of Alexandria, for approximating square roots:
>
> To approximate the square root of a positive number X,
>
> – Make a guess for the square root of X.
>
> – Compute an improved guess as the average of the guess and X divided by the guess.
>
> – Keep improving the guess until it is good enough.

That this should be so is, on reflection, not surprising. As noted earlier, the chief task for cryptographers is the development of secure methods of encryption. While the articulation of such a system in layman's English or in general mathematical terms may be useful, the devil is, at least for cryptographers, often in the algorithmic details. By utilizing source code, a cryptographer can express algorithmic ideas with precision and methodological rigor that is otherwise difficult to achieve. This has the added benefit of facilitating peer review -- by compiling the source code, a cryptographer can create a working model subject to rigorous security tests. The need for precisely articulated hypotheses and formal empirical testing, of course, is not unique to the science of cryptography; it appears, however, that in this field, source code is the preferred means to these ends.

Heron's method doesn't say anything about what square roots are, but it does say how to approximate them. This is a piece of imperative "how to" knowledge.

Computer science is in the business of formalizing imperative knowledge -- developing formal notations and ways to reason and talk about methodology. Here is Heron's method formalized as a procedure in the notation of the Lisp computer language:

```
(define (sqrtx)

(define (good-enough? guess)

 ((abs (- (square guess) x)) tolerance))

(define (improve guess)

 (average guess (/ x guess)))

(define (try guess)

 (if (good-enough? guess)

  guess

  (try (improve guess))))

(try 1))
```


[5] Thus, cryptographers use source code to express their scientific ideas in much the same way that mathematicians use equations or economists use graphs. Of course, both mathematical equations and graphs are used in other fields for many purposes, not all of which are expressive. But mathematicians and economists have adopted these modes of expression in order to facilitate the precise and rigorous expression of complex scientific ideas.13 Similarly, the undisputed record here makes it clear that cryptographers utilize source code in the same fashion.14

[6] In light of these considerations, we conclude that encryption software, in its source code form15 and as

---

13 We are reminded of at least one occasion in which a judicial thinker resorted to a mathematical equation to express a legal principle. See United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947) (Judge Hand's famous BPL formula to determine "when the absence of a bargee or other attendant will make the owner of the barge liable for injuries to other vessels if she breaks away from her moorings.").
14 Bernstein's Snuffle, in fact, provides an illustration of this point. By developing Snuffle, Bernstein was attempting to demonstrate that a one-way hash function could be employed as the heart of an encryption

method. The Snuffle source code, as submitted by Bernstein to the State Department, was meant as an expression of how this might be accomplished. The Source Code was plainly not intended as a completed encryption product, as demonstrated by the fact that it was incomplete and not in a form suitable for final compiling. The Source Code, in fact, omits the hash function entirely -- until combined with such a function and compiled, Snuffle is incapable of performing encryption functions at all.

Snuffle was also intended, in part, as political expression. Bernstein discovered that the ITAR regulations controlled encryption exports, but not one-way hash functions. Because he believed that an encryption system could easily be fashioned from any of a number of publicly-available one-way hash functions, he viewed the distinction made by the ITAR regulations as absurd. To illustrate his point, Bernstein developed Snuffle, which is an encryption system built around a one-way hash function.
15 We express no opinion regarding whether object code manifests a "close enough nexus to expression" to warrant application of the prior restraint doctrine. Bernstein's Snuffle did not involve object code, nor does the record contain any information regarding expressive uses of object code in the field of cryptography.

4234

employed by those in the field of cryptography, must be viewed as expressive for First Amendment purposes, and thus is entitled to the protections of the prior restraint doctrine. If the government required that mathematicians obtain a prepublication license prior to publishing material that included mathematical equations, we have no doubt that such a regime would be subject to scrutiny as a prior restraint. The availability of alternate means of expression, moreover, does not diminish the censorial power of such a restraint -- that Adam Smith wrote Wealth of Nations without resorting to equations or graphs surely would not justify governmental prepublication review of economics literature that contain these modes of expression.

The government, in fact, does not seriously dispute that source code is used by cryptographers for expressive purposes. Rather, the government maintains that source code is different from other forms of expression (such as blueprints, recipes, and "how-to" manuals) because it can be used to control directly the operation of a computer without conveying information to the user. In the government's view, by targeting this unique functional aspect of source code, rather than the content of the ideas that may be expressed therein, the export regulations manage to skirt entirely the concerns of the First Amendment. This argument is flawed for at least two reasons.

[7] First, it is not at all obvious that the government's view reflects a proper understanding of source code. As noted earlier, the distinguishing feature of source code is that it is meant to be read and understood by humans, and that it cannot be used to control directly the functioning of a computer. While source code, when properly prepared, can be easily compiled into object code by a user, ignoring the distinction between source and object code obscures the important fact that source code is not meant solely for the computer, but is rather written in a language intended also for human analysis and understanding.

4235

[8] Second, and more importantly, the government's argument, distilled to its essence, suggests that even one drop of "direct functionality" overwhelms any constitutional protections that expression might otherwise enjoy. This cannot be so.16 The distinction urged on us by the government would prove too much in this era of rapidly evolving computer capabilities. The fact that computers will soon be able to respond directly to spoken commands, for example, should not confer on the

government the unfettered power to impose prior restraints on speech in an effort to control its "functional " aspects. The First Amendment is concerned with expression, and we reject the notion that the admixture of functionality necessarily puts expression beyond the protections of the Constitution.

[9] The government also contends that the challenged regulations are immune from prior restraint analysis because they are "laws of general application" rather than being "directed narrowly and specifically at expression." Lakewood, 486 U.S. at 760–61. We cannot agree. Because we conclude that source code is utilized by those in the cryptography field as a means of expression, and because the regulations apply to encryption source code, it necessarily follows that the regulations burden a particular form of expression directly.

[10] The Supreme Court in Lakewood explored what it means to be a "law of general application" for prior restraint purposes. In that case, the Court cited a law requiring building permits as a "law of general application" that would not be subject to a facial attack as a prior restraint, reasoning that such a law carried "little danger of censorship, " even if it could be used to retaliate against a disfavored newspaper seeking to build a printing plant. Id. at 761. In the Court's view, "such laws provide too blunt a censorship instrument to

---

16 If it were, we would have expected the Supreme Court to start and end its analysis of David Paul O'Brien's burning of his draft card with an inquiry into whether he was kept warm by the ensuing flames. See United States v. O'Brien, 391 U.S. 367 (1968).

warrant judicial intervention prior to an allegation of actual misuse." Id. Unlike a building permit ordinance, which would afford government officials only intermittent and unpredictable opportunities to exercise unrestrained discretion over expression, the challenged EAR regulations explicitly apply to expression and place scientific expression under the censor's eye on a regular basis. In fact, there is ample evidence in the record establishing that some in the cryptography field have already begun censoring themselves, for fear that their statements might influence the disposition of future licensing applications. See, e.g., NATIONAL RESEARCH COUNCIL, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 158 (1996) ("Vendors contended that since they are effectively at the mercy of the export control regulators, they have considerable incentive to suppress any public expression of dissatisfaction with the current process."). In these circumstances, we cannot conclude that the export control regime at issue is a "law of general application" immune from prior restraint analysis.17

---

17 The government also argues that the EAR regulations are "laws of general application" because they are not purposefully aimed at suppressing any particular ideas that may be expressed in source code. With respect to this contention, the panel (including the dissenter) agree that the purpose of the regulations is irrelevant to prior restraint analysis. It is clear that a prior restraint analysis applies equally to content-neutral or content-based enactments. See FW/PBS, Inc. v. Dallas, 493 U.S. 215, 223 (1990) (plurality opinion of O'Connor, J.) ("Because we conclude that the city's licensing scheme lacks adequate procedural safeguards, we do not reach . . . whether the ordinance is properly viewed as a content-neutral time, place, and manner restriction. . . ."); Lakewood, 486 U.S. at 764 ("[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.") (emphasis in original). Indeed, where unbridled discretion is vested in a governmental official, it is difficult to know whether a licensing regime is content-based or content-neutral. Accordingly, the government's purpose in censoring encryption source code is, at this stage of our First Amendment inquiry, beside the point. In other words, a prepublication licensing regime that has a chilling and censorial effect on expression is properly subject to facial attack as a prior restraint,

4237

[11] Because the prepublication licensing scheme challenged here vests unbridled discretion in government officials, and because it directly jeopardizes scientific expression, we are satisfied that Bernstein may properly bring a facial challenge against the regulations.18 We accordingly turn to the merits.

---

whatever the purpose behind its enactment. See Lakewood, 486 U.S. at 759 (upholding facial attack against newsrack ordinance because of censorial effects, without discussing governmental purpose for enacting the ordinance).

18 It is at this juncture that we part ways with the dissent. The dissent concedes that source code can be expressive. Nevertheless, the dissent contends that Bernstein is not entitled to bring a facial attack against the EAR regulation. This argument, it seems to us, is based on two foundations.

First, the dissent conceives of the exchange of source code among scientists as "conduct." We disagree. The source code at issue here is text intended for human understanding, albeit in a specialized language. To say that the "export" of this text is "conduct " for First Amendment purposes, rather than straightforward scientific "expression," is to call into question all distribution and circulation of scientific texts that communicate ideas by using specialized languages. Of course, source code may be functional as well as expressive. We are not persuaded, however, that that fact transmogrifies the distribution of scientific texts from "expression" into "conduct" deserving of diminished First Amendment protection.

Having cast the question as one relating to "conduct," the dissent then takes a second step. Drawing from Lakeside, the dissent asks whether the "conduct" -- the exchange of cryptographic source code -- is "commonly associated with expression." This question the dissent answers in the negative; in other words, the dissent concludes that source code is not used expressively often enough. We find this conclusion somewhat perplexing, as there is nothing in the record to support it. Bernstein has introduced extensive expert evidence to support his contention that source code is frequently used for expressive purposes. The government, however, has failed to introduce anything into the record to rebut this evidence. In fact, the government has made it clear that it means to control the export of source code no matter how commonly associated it may be with expresssion: "Whatever ideas may be reflected in the software, or the intent of the exporter to convey ideas, the NSA recommends that encryption software be controlled for export solely on the basis of what it does. . . ." Second Lowell Decl., Appellant's Excerpts of Record at 104.

4238

B. Are the regulations an impermissible prior restraint?

[12] "[T]he protection even as to previous restraint is not absolutely unlimited." Near, 283 U.S. at 716. The Supreme Court has suggested that the "heavy presumption " against prior restraints may be overcome where official discretion is bounded by stringent procedural safeguards. See FW/PBS, 493 U.S. at 227 (plurality opinion of O'Connor, J.); Freedman v. Maryland, 380 U.S. 51, 58-59 (1965); Kingsley Books, 354 U.S. at 442-43; 11126 Baltimore Blvd. v. Prince George's County, 58 F.3d 988, 995 (4th Cir. 1995) (en banc). As our analysis above suggests, the challenged regulations do not qualify for this First Amendment safe harbor. 19 In Freedman v. Maryland, the Supreme Court set out three factors for determining the validity of licensing schemes that impose a prior restraint on speech: (1) any restraint must be for a specified brief period of time; (2) there must be expeditious judicial review; and (3) the censor must bear the burden of going to court to suppress the speech in question and must

---

19 The Supreme Court has also suggested that the presumption against prior restraints may be overcome where publication would directly and

imminently imperil national security. See New York Times Co. v. United States, 403 U.S. 713, 730 (1971) (Stewart, J., joined by White, J., concurring); Near, 283 U.S. at 716; see also United States v. The Progressive, Inc., 467 F. Supp. 990, 992 (W.D. Wisc. 1979). In order to justify a prior restraint on national security grounds, the government must prove the publication would "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); see also id. at 726-27 (Brennan, J., concurring) (finding that national security is a sufficient interest only 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"); Burch v. Baker, 861 F.2d 1149, 1155 (9th Cir. 1988) ("Prior restraints are permissible in only the rarest of circumstances, such as imminent threat to national security.").

The government does not argue that the prior restraint at issue here falls within the extremely narrow class of cases where publication would directly and immediately imperil national security.

4239

bear the burden of proof.20 See 380 U.S. at 58-60. The district court found that the procedural protections provided by the EAR regulations are "woefully inadequate" when measured against these requirements. Bernstein III, 974 F. Supp. at 1308. We agree.

[13] Although the regulations require that license applications be resolved or referred to the President within 90 days, see 15 C.F.R. S 750.4(a), there is no time limit once an application is referred to the President. Thus, the 90-day limit can be rendered meaningless by referral. Moreover, if the license application is denied, no firm time limit governs the internal appeals process. See 15 C.F.R. S 756.2(c)(1) (Under Secretary "shall decide an appeal within a reasonable time after receipt of the appeal."). Accordingly, the EAR regulations do not satisfy the first Freedman requirement that a licensing decision be made within a reasonably short, specified period of time. See FW/PBS, 493 U.S. at 226 (finding that "a prior restraint that fails to place time limits on the time within which the decisionmaker must issue the license is impermissible"); Riley v. National Fed. of the Blind, 487 U.S. 781, 802 (1988) (licensing scheme that permits "delay without limit" is impermissible); Vance v. Universal Amusement Co., 445 U.S. 308, 315-17 (1980) (prior restraint of indefinite duration is impermissible). The EAR regulatory regime further offends Freedman's procedural requirements insofar as it denies a disappointed applicant the opportunity for judicial review.21 See

---

20 Whether all three Freedman factors apply to all prior restraints is the subject of dispute. Compare FW/PBS, 493 U.S. at 229-30 (plurality opinion of O'Connor, J.) (finding the government does not bear the burden of going to court to defend its licensing requirement where restrained speakers are likely to challenge the restraint in court) with id. at 239 (Brennan, J., concurring in judgment) ("We have never suggested that our insistence on Freedman procedures might vary with the particular facts of the prior restraint before us."). Because we conclude that the EAR regulations fail Freedman's first two procedural requirements, we need not reach the issue of whether the third Freedman factor applies in this case.

21 As noted earlier, the BXA enjoys essentially unbounded discretion under the EAR regulations in administering the license process. Accord-

4240

15 C.F.R. S 756.2(c)(2); FW/PBS, 493 U.S. at 229 (plurality opinion of O'Connor, J.) (finding failure to provide "prompt" judicial review violates Freedman); Freedman, 380 U.S. at 59 (licensing procedure must assure a prompt final judicial decision).

[14] We conclude that the challenged regulations allow the

government to restrain speech indefinitely with no clear criteria for review. As a result, Bernstein and other scientists have been effectively chilled from engaging in valuable scientific expression. Bernstein's experience itself demonstrates the enormous uncertainty that exists over the scope of the regulations and the potential for the chilling of scientific expression. In short, because the challenged regulations grant boundless discretion to government officials, and because they lack the required procedural protections set forth in Freedman, we find that they operate as an unconstitutional prior restraint on speech.22 See Lakewood, 486 U.S. at 769-772 (holding that newsrack licensing ordinance was an impermissible prior restraint because it conferred unbounded discretion and lacked adequate procedural safeguards).

---

ingly, even if the challenged regulations provided for judicial review, the lack of explicit limits on the decisionmaker's discretion would likely make such review meaningless. In this sense, the presence of unbounded discretion itself may be considered fatal for purposes of prior restraint review. See Lakewood, 486 U.S. at 769-70 (striking down a licensing scheme where the mayor could merely claim that the license" `is not in the public interest' when denying a permit application").

22 Our conclusion relating to the Source Code also resolves the status of the regulations as applied to the Instructions. Because the Instructions are essentially a translation of the Source Code into English, they are, if anything, nearer the heartland of the First Amendment. Consequently, to the extent the challenged regulations are unconstitutional as applied to the Source Code, they necessarily are unconstitutional as applied to the Instructions.

4241

C. Concluding comments.

We emphasize the narrowness of our First Amendment holding. We do not hold that all software is expressive. Much of it surely is not. Nor need we resolve whether the challenged regulations constitute content-based restrictions, subject to the strictest constitutional scrutiny, or whether they are, instead, content-neutral restrictions meriting less exacting scrutiny. We hold merely that because the prepublication licensing regime challenged here applies directly to scientific expression, vests boundless discretion in government officials, and lacks adequate procedural safeguards, it constitutes an impermissible prior restraint on speech.

We will, however, comment on two issues that are entwined with the underlying merits of Bernstein's constitutional claims. First, we note that insofar as the EAR regulations on encryption software were intended to slow the spread of secure encryption methods to foreign nations, the government is intentionally retarding the progress of the flourishing science of cryptography. To the extent the government's efforts are aimed at interdicting the flow of scientific ideas (whether expressed in source code or otherwise), as distinguished from encryption products, these efforts would appear to strike deep into the heartland of the First Amendment. In this regard, the EAR regulations are very different from content-neutral time, place and manner restrictions that may have an incidental effect on expression while aiming at secondary effects.

Second, we note that the government's efforts to regulate and control the spread of knowledge relating to encryption may implicate more than the First Amendment rights of cryptographers. In this increasingly electronic age, we are all required in our everyday lives to rely on modern technology to communicate with one another. This reliance on electronic communication, however, has brought with it a dramatic diminution in our ability to communicate privately. Cellular

4242

phones are subject to monitoring, email is easily intercepted, and transactions over the internet are often less than secure. Something as commonplace as furnishing our credit card number, social security number, or bank account number puts each of us at risk. Moreover, when we employ electronic methods of communication, we often leave electronic "fingerprints" behind, fingerprints that can be traced back to us. Whether we are surveilled by our government, by criminals, or by our neighbors, it is fair to say that never has our ability to shield our affairs from prying eyes been at such a low ebb. The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost. Government efforts to control encryption thus may well implicate not only the First Amendment rights of cryptographers intent on pushing the boundaries of their science, but also the constitutional rights of each of us as potential recipients of encryption's bounty. Viewed from this perspective, the government's efforts to retard progress in cryptography may implicate the Fourth Amendment, as well as the right to speak anonymously, see McIntyre v. Ohio Elections Comm'n, 115 S. Ct. 1511, 1524 (1995) , the right against compelled speech, see Wooley v. Maynard, 430 U.S. 705, 714 (1977), and the right to informational privacy, see Whalen v. Roe, 429 U.S. 589, 599–600 (1977). While we leave for another day the resolution of these difficult issues, it is important to point out that Bernstein's is a suit not merely concerning a small group of scientists laboring in an esoteric field, but also touches on the public interest broadly defined.

II. Scope of Declaratory Relief

The government also challenges the scope of the declaratory relief granted by the district court. The government argues that the relief provided is invalid in two respects: (1) that the relief extends to encryption object code and encryption commodities; (2) that the relief extends to encryption technology. The district held that

> the Export Administration Regulations, 15 C.F.R. pt. 730 et seq. (1997) and all rules, policies and practices promulgated or pursued thereunder insofar as they apply to or require licensing for encryption and decryption software and related devices and technology are in violation of the First Amendment on the grounds of prior restraint and are, therefore, unconstitutional as discussed above, and shall not be applied to plaintiff's publishing of such items, including scientific papers, algorithms or computer programs.

Bernstein III, 974 F. Supp. at 1310. We review the district court's grant of declaratory relief de novo. See Crawford v. Lungren, 96 F.3d 380, 384 (9th Cir. 1996); Ablang v. Reno, 52 F.3d 801, 803 (9th Cir. 1995).

This inquiry leads us into the uncertain jurisprudence of "severability." See generally John Copeland Nagle, Severability, 72 N.C. L. REV. 203 (1993). The general principle is clear: "[A] court should refrain from invalidating more of [a] statute than is necessary . . . . `[W]henever an act of Congress contains unobjectionable provisions separable from those found to be unconstitutional, it is the duty of this court to so declare, and to maintain the act in so far as it is valid.' " Alaska Airlines, Inc. v. Brock, 480 U.S. 678, 684 (1987) (quoting Regan v. Time, Inc., 468 U.S. 641, 652 (1984)); see also National Collegiate Athletic Ass'n v. Miller , 10 F.3d 633, 640 (9th Cir. 1993). The applicable legal standard has also been oft repeated: "[u]nless it is evident that the Legislature would not have enacted those provisions which are within its

power, independently of that which is not, the invalid part may be dropped if what is left is fully operative as a law." Buckley v. Valeo, 424 U.S. 1, 108 (1976) (per curiam); accord NCAA v. Miller, 10 F.3d at 640. Thus, in the general case, severability analysis properly focuses on legislative intent. See Alaska Airlines, Inc., 480 U.S. at 685.

4244

This case, however, is not the general case. First, the challenged enactment here is a regulation, rather than a statute. As a result, we cannot look to the usual public sources to determine the intentions of the drafters. Nevertheless, we agree with the government that the EAR regulations can be conceptually severed into component parts governing commodities, software, and technology. We also assume that the Department of Commerce, even if barred from imposing prepublication licensing on encryption source code, would have enacted regulations controlling the export of encryption commodities, object code, and technology.

But while the district court may have erred in treating software and commodities as the same item, the integrated structure of the regulations does not permit us to sever the various provisions in the manner requested by the government. To sever the unconstitutional portion of the regulations, we would have to line edit individual sections, deleting or modifying the definition of "software" while retaining "commodities" and "technology." We would then have to redefine general terms such as "items" which refer collectively to commodities, software, and technology. We have neither the power nor the capacity to engage in line by line revisions of the challenged regulations or to redefine terms within the regulations. See Hill v. Wallace, 259 U.S. 44, 70–71 (1922); American Booksellers Ass'n v. Hudnut, 771 F.2d 323, 332–33 (7th Cir. 1985). To do so would be to improperly invade the province reserved to the Executive. Accordingly, we affirm the district court's grant of declaratory relief.

CONCLUSION

Because the prepublication licensing regime challenged by Bernstein applies directly to scientific expression, vests boundless discretion in government officials, and lacks adequate procedural safeguards, we hold that it constitutes an impermissible prior restraint on speech. We decline the invitation to line edit the regulations in an attempt to rescue them

4245

from constitutional infirmity, and thus endorse the declaratory relief granted by the district court.

AFFIRMED.

BRIGHT, Circuit Judge, separately concurring.

I join Judge Fletcher's opinion. I do so because the speech aspects of encryption source code represent communication between computer programmers. I do, however, recognize the validity of Judge Nelson's view that encryption source code also has the functional purpose of controlling computers and in that regard does not command protection under the First Amendment. The importance of this case suggests that it may be appropriate for review by the United States Supreme Court.

T.G. NELSON, Circuit Judge, Dissenting:

Bernstein was not entitled to bring a facial First Amendment challenge to the EAR, and the district court improperly granted an injunction on the basis of a facial challenge. I therefore respectfully dissent.

The basic error which sets the majority and the district court adrift is the failure to fully recognize that the basic function of encryption source code is to act as a method of controlling computers. As defined in the EAR regulations, encryption source code is "[a] precise set of operating instructions to a computer, that when compiled, allows for the execution of an encryption function on a computer." 15 C.F.R. pt. 722. Software engineers generally do not create software in object code--the series of binary digits (1's and 0's)--which tells a computer what to do because it would be enormously

4246

difficult, cumbersome and time-consuming. Instead, software engineers use high-level computer programming languages such as "C" or "Basic" to create source code as a shorthand method for telling the computer to perform a desired function. In this respect, lines of source code are the building blocks or the tools used to create an encryption machine. See e.g., Patrick Ian Ross, Bernstein v. United States Department of State, 13 Berkeley Tech. L.J. 405, 410-11 (1998) ("[E]lectronic source code that is ready to compile merely needs a few keystrokes to generate object code--the equivalent of flipping an `on' switch. Code used for this purpose can fairly easily be characterized as `essentially functional.' "); Pamela Samuelson et al., A Manifesto Concerning Legal Protection of Computer Programs, 94 Colum. L. Rev. 2308, 2315-30 (1994) ("[P]rograms are, in fact, machines (entities that bring about useful results, i.e., behavior) that have been constructed in the medium of text (source code and object code)."). Encryption source code, once compiled, works to make computer communication and transactions secret; it creates a lockbox of sorts around a message that can only be unlocked by someone with a key. It is the function or task that encryption source code performs which creates its value in most cases. This functional aspect of encryption source code contains no expression; it is merely the tool used to build the encryption machine.

This is not to say that this very same source code is not used expressively in some cases. Academics, such as Bernstein, seek to convey and discuss their ideas concerning computer encryption. As noted by the majority, Bernstein must actually use his source code textually in order to discuss or teach cryptology. In such circumstances, source code serves to express Bernstein's scientific methods and ideas.

While it is conceptually difficult to categorize encryption source code under our First Amendment framework, I am still inevitably led to conclude that encryption source code is more like conduct than speech. Encryption source code is a building

4247

tool. Academics and computer programmers can convey this source code to each other in order to reveal the encryption machine they have built. But, the ultimate purpose of encryption code is, as its name suggests, to perform the function of encrypting messages. Thus, while encryption source code may occasionally be used in an expressive manner, it is inherently a functional device.

We are not the first to examine the nature of encryption

source code in terms of First Amendment protection. Judge Gwin of the United States District Court for the Northern District of Ohio also explored the function versus expression conundrum of encryption source code at some length in Junger v. Daley, 8 F. Supp. 2d 708 (N.D. Ohio 1998). Junger, like Bernstein, is a professor, albeit a law professor, who wished to publish in various forms his work on computers, including a textbook, Computers and the Law. The book was determined by the Government to be subject to export without a license, but his software programs were determined to come within the licensing provisions of the EAR. In the course of rejecting Junger's claims, the court said:

> Like much computer software, encryption source code is inherently functional; it is designed to enable a computer to do a designated task. Encryption source code does not merely explain a cryptographic theory or describe how the software functions. More than describing encryption, the software carries out the function of encryption. The software is essential to carry out the function of encryption. In doing this function, the encryption software is indistinguishable from dedicated computer hardware that does encryption.
>
> In the overwhelming majority of circumstances, encryption source code is exported to transfer functions, not to communicate ideas. In exporting functioning capability, encryption source code is like

> other encryption devices. For the broad majority of persons receiving such source code, the value comes from the function the source code does.

Id. at 716. The Junger decision thus adds considerable support for the propositions that encryption source code cannot be categorized as pure speech and that the functional aspects of encryption source code cannot be easily ignored or put aside.

Both the district court and the majority hold that because source code can be used expressively in some circumstances, Bernstein was entitled to bring a facial challenge to the EAR. Such an approach ignores the basic tenet that facial challenges are inappropriate "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) (quoting City of Lakewood v. Plain Dealer Publishing Co., 486 U.S. 750, 760 (1988)). That encryption source code may on occasion be used expressively does not mean that its export is "conduct commonly associated with expression" or that the EAR regulations are directed at expressive conduct. See id. at 303 ("The fact that sitting can possibly be expressive, however, isn't enough to sustain plaintiffs' facial challenge."); see also Junger, 8 F. Supp. 2d at 718 ("[T]he prior restraint doctrine is not implicated simply because an activity may on occasion be expressive.").

The activity or conduct at issue here is the export of encryption source code. As I noted above, the basic nature of encryption source code lies in its functional capacity as a method to build an encryption device. Export of encryption source code is not conduct commonly associated with expression. Rather, it is conduct that is normally associated with providing other persons with the means to make their computer messages secret. The overwhelming majority of people do not want to talk about the source code and are not inter-

ested in any recondite message that may be contained in encryption source code. Only a few people can actually understand what a line of source code would direct a computer to do. Most people simply want to use the encryption source code to protect their computer communications. Export of encryption source code simply does not fall within the bounds of conduct commonly associated with expression such as picketing or handbilling. See Roulette, 97 F.3d at 303–04.

Further, the EAR regulates the export of encryption technology generally, whether it is software or hardware. See 15 C.F.R. S 742.15; Junger, 8 F. Supp. 2d at 718 ("The Export Regulations do not single out encryption software."). These regulations are directed at preventing the functional capacity of any encryption device, including its source code, from being exported without a government license. The EAR is not specifically directed towards stifling the expressive nature of source code or Bernstein's academic discussions about cryptography. This is demonstrated by the fact that the regulations do not object to publication in printed form of learned articles containing source code. See 15 C.F.R. S 734.3. Thus, the EAR is generally directed at non–expressive conduct––the export of source code as a tool to make messages secret and impervious to government eavesdropping capabilities.

Because this is a law of general application focused at conduct, Bernstein is not entitled to bring a facial challenge. The district court's injunction based upon the finding of a facial prior restraint is thus impermissible. This is not to say that Bernstein's activities would not be entitled to First Amendment protection, but that the legal path chosen to get that protection must be the correct one. We should be careful to "entertain[ ] facial freedom–of–expression challenges only against statutes that, `by their terms,' sought to regulate `spoken words,' or patently `expressive or communicative conduct.' " Roulette, 97 F.3d at 303 (citing Broadrick v. Oklahoma, 413 U.S. 601, 612–13 (1973)). Bernstein may very well have a claim under an as–applied First Amendment anal–

ysis; however, such a claim must be left to the district court's determination in the first instance. Here, the district court did not rule on Bernstein's as–applied claims. I would therefore vacate the district court's injunction and remand for consideration of Bernstein's as–applied challenges to the EAR. Accordingly, I respectfully dissent.