176 F.3d 1132

United States Court of Appeals,

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.

Argued and Submitted Dec. 8, 1997.Decided May 6, 1999.

Mathematician brought action challenging constitutionality of International Traffic in Arms Regulations (ITAR), which restricted mathematician's ability to distribute his encryption software. The United States District Court for the Northern District of California, 922 F.Supp. 1426, found that mathematician's source code was protected speech, and subsequently, 945 F.Supp. 1279, granted summary judgment for mathematician on First Amendment claims. After licensing authority for nonmilitary encryption commodities and technologies was shifted to Department of Commerce, mathematician amended complaint to raise same challenges to Department's new Export Administration Regulations (EAR). The District Court, Marilyn Hall Patel, J., 974 F.Supp. 1288, granted summary judgment for mathematician and enjoined Commerce Department from future enforcement of invalidated provisions. Government appealed. The Court of Appeals, Betty B. Fletcher, Circuit Judge, held that: (1) encryption software, in its source code form and as employed by those in the field of cryptography, is expression for First Amendment purposes; (2) mathematician could bring facial challenge against regulations on prior restraint grounds; and (3) regulations imposed prior restraint that violated First Amendment.

Affirmed.

Opinion

Opinion by Judge Betty B. FLETCHER; Concurrence by Judge BRIGHT; Dissent by Judge T.G. NELSON.

Betty 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 University of California, Berkeley, he developed an encryption method—"a zero-delay private-key stream encryptor based upon a one-way hash function"[1]— ***1136*** 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 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. U.S. 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. U.S. 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. U.S. Department of State,* 974 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 KAHN, THE CODEBREAKERS (2d ed.1996). For much of ****1137*** 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 foreign 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 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 ***1138** 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 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. § 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. § 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. § 756.2(c)(1). Final administrative decisions are not subject to judicial review. 15 C.F.R. § 756.2(c)(2).

DISCUSSION

I. Prior Restraint

1The 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).

2It 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, 96 S.Ct. 2791, 49 L.Ed.2d 683 (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, 51 S.Ct. 625, 75 L.Ed. 1357 (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, 91 S.Ct. 1575, 29 L.Ed.2d 1 (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, 77 S.Ct. 1325, 1 L.Ed.2d 1469 (1957). We accordingly turn from "[t]he generalization that prior restraint is particularly obnoxious" to a "more particularistic analysis." *Id.* at 442.

***1139** 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, 108 S.Ct. 2138, 100 L.Ed.2d 771 (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?

345A licensing regime is always subject to facial challenge[8] 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.

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. § 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.

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]

***1140** 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 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] That this should be so is, on reflection, not surprising. As noted ***1141** 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.

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]

6In light of these considerations, we conclude that encryption software, in its source code form[15] and as 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 ***1142*** 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.

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.

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.

7The 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.

8910The 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 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 ***1143*** 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]

11Because 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.

B. Are the regulations an impermissible prior restraint?

1213"[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* ***1144** *FW/PBS,* 493 U.S. at 227 (plurality opinion of O'Connor, J.); *Freedman v. Maryland,* 380 U.S. 51, 58–59, 85 S.Ct. 734, 13 L.Ed.2d 649 (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 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.

Although the regulations require that license applications be resolved or referred to the President within 90 days, *see* 15 C.F.R. § 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. § 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, 108 S.Ct. 2667, 101 L.Ed.2d 669 (1988)(licensing scheme that permits "delay without limit" is impermissible); *Vance v. Universal Amusement Co.,* 445 U.S. 308, 315–17, 100 S.Ct. 1156, 63 L.Ed.2d 413 (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* ***1145** 15 C.F.R. § 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).

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).

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 phones are subject to monitoring, email is easily intercepted, and ***1146** 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,* 514 U.S. 334, 115 S.Ct. 1511, 1524, 131 L.Ed.2d 426 (1995), the right against compelled speech, *see* *Wooley v. Maynard,* 430 U.S. 705, 714, 97 S.Ct. 1428, 51 L.Ed.2d 752 (1977), and the right to informational privacy, *see* *Whalen v. Roe,* 429 U.S. 589, 599–600, 97 S.Ct. 869, 51 L.Ed.2d 64 (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

1415The 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).

1617This inquiry leads us into the uncertain jurisprudence of “severability.” *See generally* John Copeland Nagle, *Severability,* 72N.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, 107 S.Ct. 1476, 94 L.Ed.2d 661 (1987) (quoting *Regan v. Time, Inc.,* 468 U.S. 641, 652, 104 S.Ct. 3262, 82 L.Ed.2d 487 (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, 96 S.Ct. 612, 46 L.Ed.2d 659 (1976) (per curiam); *accord* *NCAA v. Miller,* 10 F.3d at 640. Thus, in ***1147** the general case, severability analysis properly focuses on legislative intent. *See* *Alaska Airlines, Inc.,* 480 U.S. at 685.

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, 42 S.Ct. 453, 66 L.Ed. 822 (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 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 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 ***1148** 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 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.

***1149** *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, 108 S.Ct. 2138, 100 L.Ed.2d 771 (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 interested 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. § 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. § 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, 93 S.Ct. 2908, 37 L.Ed.2d 830 (1973)). Bernstein may very well have a claim under an as-applied First Amendment analysis; however, such a claim must be left to the district court's ***1150** 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.