

3 of 283 DOCUMENTS

Peter D. Junger, Plaintiff-Appellant, v. William Daley, United States Secretary of Commerce, et al., Defendants-Appellees.

No. 98-4045

UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

209 F.3d 481; 2000 U.S. App. LEXIS 6161; 2000 FED App. 0117P (6th Cir.); 28 Media L. Rep. 1609

December 17, 1999, Argued

April 4, 2000, Decided

April 4, 2000, Filed

PRIOR HISTORY:

[**1] Appeal from the United States District Court for the Northern District of Ohio at Akron. No. 96-01723. James S. Gwin, District Judge.

DISPOSITION:

REVERSED district court and REMANDED case to the district court for consideration of Junger's constitutional challenge to the amended regulations.

COUNSEL:

ARGUED: Gino J. Scarselli, ACLU OF OHIO FOUNDATION, Cleveland, Ohio, for Appellant.

Scott R. McIntosh, U.S. DEPARTMENT OF JUSTICE, CIVIL DIVISION, APPELLATE STAFF, Washington, D.C., for Appellees.

ON BRIEF: Gino J. Scarselli, Raymond Vasvari, ACLU OF OHIO FOUNDATION, Cleveland, Ohio, Kevin F. O'Neill, CLEVELAND-MARSHALL COLLEGE OF LAW, Cleveland, Ohio, for Appellant.

Scott R. McIntosh, U.S. DEPARTMENT OF JUSTICE, CIVIL DIVISION, APPELLATE STAFF, Washington, D.C., for Appellees.

David W. Addis, Kurt A. Wimmer, COVINGTON & BURLING, Washington, D.C., Robert M. O'Neil, J. Joshua Wheeler, THOMAS JEFFERSON CENTER FOR THE PROTECTION OF FREE EXPRESSION, Charlottesville, Virginia, Paul F. Gamble, Bloomfield Hills, Michigan, for Amici Curiae.

JUDGES:

Before: MARTIN, Chief Judge; CLAY, Circuit Judge; WEBER, District Judge. *

* Honorable Herman J. Weber, United States District Judge for the Southern District of Ohio, sitting by designation. [**2]

OPINIONBY:

BOYCE F. MARTIN, JR.

OPINION:

[*482]

BOYCE F. MARTIN, JR., Chief Judge. This is a constitutional challenge to the provisions of the Export Administration Regulations, 15 C.F.R. Parts 730-74, that regulate the export of encryption software. Peter D. Junger appeals the district court's grant of summary judgment in favor of Secretary Daley and the other defendants.

The district court found that encryption source code is not sufficiently expressive to be protected by the First Amendment, that the Export Administration Regulations are permissible content-neutral restrictions, and that the Regulations are not subject to a facial challenge as a prior restraint on speech. Subsequent to the district court's holding and the oral arguments before this Court, the Bureau of Export Administration issued an interim final rule amending the regulations at issue. See Revisions to Encryption Items, 65 Fed. Reg. 2492 (2000) (to be codified at 15 C.F.R. Parts 734, 740, 742, 770, 772, 774). Having concluded that the First Amendment protects computer source code, we reverse the district court and remand this case for further consideration of Junger's constitutional claims [**3] in light of the amended regulations.

ENCRYPTION AND SOFTWARE BACKGROUND

Encryption is the process of converting a message from its original form ("plaintext") into a scrambled form ("ciphertext"). Most encryption today uses an algorithm, a mathematical transformation from plaintext to ciphertext, and a key that acts as a password. Generally, the security of the message depends on the strength of both the algorithm and the key.

Encryption has long been a tool in the conduct of military and foreign affairs. Encryption has many civil applications, including protecting communication and data sent over the Internet. As technology has progressed, the methods of encryption have changed from purely mechanical processes, such as the Enigma machines of Nazi Germany, to modern electronic processes. [*483] Today, messages can be encrypted through dedicated electronic hardware and also through general-purpose computers with the aid of encryption software.

For a general-purpose computer to encrypt data, it must use encryption software that instructs the

computer's circuitry to execute the encoding process. Encryption software, like all computer software, can be in one of two forms: object code [**4] or source code. Object code represents computer instructions as a sequence of binary digits (0s and 1s) that can be directly executed by a computer's microprocessor. Source code represents the same instructions in a specialized programming language, such as BASIC, C, or Java. Individuals familiar with a particular computer programming language can read and understand source code. Source code, however, must be converted into object code before a computer will execute the software's instructions. This conversion is conducted by compiler software. Although compiler software is typically readily available, some source code may have no compatible compiler.

REGULATORY BACKGROUND

The Export Administration Regulations create a comprehensive licensing scheme to control the export of nonmilitary technology, software, and commodities. In 1996, the President transferred export jurisdiction over nonmilitary encryption items from the State Department to the Commerce Department's Bureau of Export Administration.

The Regulations are structured around the Commodity Control List, which lists items subject to export control. See 15 C.F.R. Part 774. Each item on the List is given [**5] an Export Control Classification Number that designates the category of the controlled item and the reasons why the government controls the item's export. See 15 C.F.R. § 738.2. The reasons for control affect the nature and scope of the export controls.

Encryption software, including both source code and object code, is regulated under Export Control Classification Number 5D002 for national security reasons. See *id.* § 772 Supp. 1. In addition, encryption technology and encryption hardware are regulated for national security reasons under different Classification Numbers. Generally, the Regulations require a license for the export of all encryption items to all foreign destinations, except Canada. See 65 Fed. Reg. 2492, 2499 (to be codified at 15 C.F.R. § 742.15(a)). Although the regulations provide some exceptions, most encryption software in electronic form remains subject to the license requirements for export. Encryption software in printed form, however, is not subject to the Regulations. See 15 C.F.R. § 734.3(b)(2).

The Regulations define "export" as the "actual shipment or transmission of items subject to the EAR out of the United States. [**6]" *Id.* § 734.2(b)(1). For encryption software, the definition of "export" also includes publication of the software on the Internet, unless steps are taken to restrict foreign access to the Internet site. See 65 Fed. Reg. 2492, 2496 (to be codified at 15 C.F.R. § 734.2(b)(9)(ii)).

FACTUAL BACKGROUND

Peter Junger is a professor at the Case Western University School of Law. Junger maintains sites on the World Wide Web that include information about courses that he teaches, including a computers and the law course. Junger wishes to post on his web site encryption source code that he has written to demonstrate how computers work. Such a posting is defined as an export under the Regulations.

On June 12, 1997, Junger submitted three applications to the Commerce Department, requesting determinations of commodity classifications for encryption software programs and other items. On July 4, the Export Administration told Junger that Classification Number 5D002 covered four of the five software programs [*484] he had submitted. Although it found that four programs were subject to the Regulations, the Export Administration found that the first chapter of Junger's [**7] textbook, *Computers and the Law*, was an allowable unlicensed export. Though deciding that the printed book chapter containing encryption code could be exported, the Export Administration stated that export of the book in electronic form would require a license if the text contained 5D002 software. Since receiving the classification determination, Junger has not applied for a license to export his classified encryption source code.

Junger filed this action to make a facial challenge to the Regulations on First Amendment grounds, seeking declaratory and injunctive relief that would permit him to engage in the unrestricted distribution of encryption software through his web site. Junger claims that encryption source code is protected speech. The district court granted summary judgment in favor of the defendants, holding that encryption source code is not protected under the First Amendment, that the Regulations are permissible content-neutral regulations, and that the Regulations are not subject to facial challenge on prior restraint grounds.

We review the grant of summary judgment de novo. See *Smith v. Wal-Mart Stores, Inc.*, 167 F.3d 286, 289 (6th Cir. 1999). [**8]

The issue of whether or not the First Amendment protects encryption source code is a difficult one because source code has both an expressive feature and a functional feature. The United States does not dispute that it is possible to use encryption source code to represent and convey information and ideas about cryptography and that encryption source code can be used by programmers and scholars for such informational purposes. Much like a mathematical or scientific formula, one can describe the function and design of encryption software by a prose explanation; however, for individuals fluent in a computer programming language, source code is the most efficient and precise means by which to communicate ideas about cryptography.

The district court concluded that the functional characteristics of source code overshadow its simultaneously expressive nature. The fact that a medium of expression has a functional capacity should not preclude constitutional protection. Rather, the appropriate consideration of the medium's functional capacity is in the analysis of permitted government regulation.

The Supreme Court has explained that "all ideas having even the slightest redeeming social importance, [**9] " including those concerning "the advancement of truth, science, morality, and arts" have the full protection of the First Amendment. *Roth v. United States*, 354 U.S. 476, 484, 1 L. Ed. 2d 1498, 77 S. Ct. 1304 (1957) (quoting 1 *Journals of the Continental Congress* 108 (1774)). This protection is not reserved for purely expressive communication. The Supreme Court has recognized First Amendment protection for symbolic conduct, such as draft-card burning, that has both functional and expressive features. See *United States v. O'Brien*, 391 U.S. 367, 20 L. Ed. 2d 672, 88 S. Ct. 1673 (1968).

The Supreme Court has expressed the versatile scope of the First Amendment by labeling as "unquestionably shielded" the artwork of Jackson Pollack, the music of Arnold Schoenberg, or the Jabberwocky verse of Lewis Carroll. *Hurley v. Irish-American Gay, Lesbian and Bisexual Group*, 515 U.S. 557, 569, 132 L. Ed. 2d 487, 115 S. Ct. 2338 (1995). Though unquestionably expressive, these things identified by the Court are not traditional speech. Particularly, a musical score cannot be read by the majority of the public but can be used as a means **[**10]** of communication among musicians. Likewise, computer source code, though unintelligible to many, is the preferred method of communication among computer programmers. **[*485]**

Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment.

The functional capabilities of source code, and particularly those of encryption source code, should be considered when analyzing the governmental interest in regulating the exchange of this form of speech. Under intermediate scrutiny, the regulation of speech is valid, in part, if "it furthers an important or substantial governmental interest." *O'Brien*, 391 U.S. at 377. In *Turner Broadcasting System v. FCC*, 512 U.S. 622, 664, 129 L. Ed. 2d 497, 114 S. Ct. 2445 (1994), the Supreme Court noted that although an asserted governmental interest may be important, when the government defends restrictions on speech "it must do more than simply 'posit the existence of the disease sought to be cured.'" *Id.* (quoting *Quincy Cable TV, Inc. v. FCC*, 248 U.S. App. D.C. 1, 768 F.2d 1434, 1455 (D.C. Cir. 1985)). **[**11]** The government "must demonstrate that the recited harms are real, not merely conjectural, and that the regulation will in fact alleviate these harms in a direct and material way." *Id.* We recognize that national security interests can outweigh the interests of protected speech and require the regulation of speech. In the present case, the record does not resolve whether the exercise of presidential power in furtherance of national security interests should overrule the interests in allowing the free exchange of encryption source code.

Before any level of judicial scrutiny can be applied to the Regulations, Junger must be in a position to bring a facial challenge to these regulations. In light of the recent amendments to the Export Administration Regulations, the district court should examine the new regulations to determine if Junger can bring a facial challenge.

For the foregoing reasons, we REVERSE the district court and REMAND the case to the district court for consideration of Junger's constitutional challenge to the amended regulations.