Encryption Technology And First Amendment Rights

Roy Whitehead, Jr, (E-mail: royw@mail.uca.edu), University of Central Arkansas
Ken Griffin, (E-mail: keng@mail.uca.edu), University of Central Arkansas
Paul Jensen, (E-mail: paulj@mail.uca.edu), University of Central Arkansas

Abstract

The predicated enormous boom in electronic commerce will only flower when users are assured that their electronic transmissions are secure. To assure this security, encryption technology must be powerful and difficult to decipher. Unfortunately, for electronic visionaries, U.S. law prevents powerful encryption programs from being exported, posted on the Internet, or otherwise communicated to persons who might take the technology outside our borders, unless an export license is first obtained. Such license will be denied unless the key link is less than a weak 56 bits and the potential exporter places a key to perform encryption of the program in escrow for the government. The government seeks to justify this restraint on export by raising national security concerns that terrorists or foreign military forces will adopt the encryption systems. This licensing requirement, however, is viewed as an unacceptable burden on electronic commerce by both developers and potential domestic and foreign users of sophisticated encryption technology. This article discusses a precedent setting recent case that attempted to reconcile the conflicting encryption technology interests of scientists, scholars, users, and the government. The court wisely balanced the competing interests and decided that, while the government can regulate the export of encryption technology, it must do so within the bounds of the scientist and scholar's First Amendment rights of teaching, discussion, and expression.

Introduction

By the year 2000, annual purchases made over the world-wide web are estimated to reach a total value of 78 billion U.S. dollars. This boom in E-commerce can occur, however, only if the electronic transactions are secure. Encryption technology can provide this required security. Through the use of public key encryption, a seller of goods over the Internet can ensure that an order was placed by the person from whom it was supposed to come, that the order has not be tampered with, and that the

customer cannot later change the terms of the offer by claiming that he was actually offered a lower price. Importantly, the terms of the offer can also be kept confidential from other parties.

To assure this security, encryption technology must be powerful and difficult to crack. Unfortunately, U.S. law prevents powerful encryption programs from being sold outside the United States, posted on the Internet, or otherwise communicated to non-citizens who might take the programs outside the U.S., unless an export license is first obtained. Such license will be denied unless the key link does not exceed 56

Readers with comments or questions are encouraged to contact the authors via e-mail.

bits. Consequently, the program cannot be very powerful.

In addition, any prospective exporter of encryption technology must agreed to arrange for a key recovery mechanism. The exporter must place the keys required to perform decryption of the message in escrow with a trustworthy commercial enterprise. If the Government has reason to believe that the encryption products are being used for unlawful purposes, and can get a court order permitting to do so, it can obtain the keys and decrypt the messages. This requirement is not popular among potential purchasers of encryption technology, particularly those in Europe and the Far East. As a result, the United States recently attempted to bar a research and assistant professor at the University of Illinois at Chicago, from even talking or writing about his encryption software. This article discusses the resulting case of *Bernstein v. U.S. Department of State*, No. C-95-1-0592 (N.D. Cal. 1997).

Overview of Bernstein Case

Daniel Bernstein, currently a Research Assistant Professor in the Department of Mathematics, Statistics and Computer Science at the University of Illinois at Chicago, originally brought this action against the Department of State and others seeking declaratory and injunctive relief from their enforcement of the Arms Export Control Act (AECA) [22 U.S.C. Section 2778 (1990)], and the International Traffic in Arms Regulations (ITAR) [22 C.F.R. section 120 (1994)], on the grounds that the regulations were an unconstitutional abridgement of the freedom of speech and expression. The court granted some relief on December 9, 1996, when it decided that his computer codes were protected speech and the Department of State licensing requirements were an unlawful prior restraint of Bernsteins's freedom of expression. However, just prior to the court's order, President Clinton, by Executive Order 13026, transferred jurisdiction over the export of non-military encryption technology products to the Department of Commerce pursuant to the Export Administration Act of 1979 (EAA), and the Export Administration

Regulations (EAR). On December 30, 1996, the Commerce Department issued an interim rule regulating the export of certain encryption products [61 Fed. Reg. 68572 (Dec. 30, 1996)]. The new regulations cleverly attempted to characterize Bernstein's encryption computer codes as "functional" engines that drive his program rather than an "expression" of his ideas subject to First Amendment protection. Consequently, Bernstein was required to amend his complaint to include the new regulations and new defendants. Thereafter, the court considered the question of whether the licensing requirements for the export of cryptographic devices, software and related technology covered by the amendments to the EAR constitute an impermissible infringement on speech in violation of the First Amendment.

Encryption And National Security

Encryption involves running a readable message known as "plain text" through a computer program that translates a message according to an equation algorithm into unreadable "cipher text." Decryption is the translation back to plain text when the message is received by someone with an appropriate "key." The message is both encrypted and decrypted by compatible keys. The uses of cryptography are far ranging in the electronic age, from protecting personal messages over the Internet and transactions on bank ATMs to ensuring the secrecy of military intelligence. In a prepublication copy of a report prepared by the National Research Council (NRC) at the request of the Defense Department, the NRC identified four major uses of cryptography: ensuring data integrity; authenticating users; facilitating nonrepudiation (the linking of a specific message with a specific sender) and maintaining confidentiality.

Once a field dominated almost exclusively by governments concerned with protecting their own secrets as well as accessing information held by others, the last twenty years has seen the popularization of cryptography as industries and individuals alike have increased their use of electronic media and have sought to protect their electronic products and communica-

tions. However, potential defense articles and defense services are identified on a United States Munitions List (USML) [22 U.S.C. 2778 (b) (2)] and require a license before they can be imported or exported. All cryptographic systems and software have been designated as a munitions item. The ITAR allows for a commodity jurisdiction procedure" by which the Office of Defense Trade Controls (ODTC) determines if an article or service is covered by the USML when doubt exists about an item.

The Encryption Technology: Snuffles"

Cryptography has become a dynamic academic discipline within applied mathematics and is the subject of considerable academic writing and conference discussion. As a graduate student, Bernstein developed an encryption algorithm he calls "Snuffle." He describes Snuffle as a zero- delay private-key encryption system. Bernstein has articulated his mathematical ideas in two ways: in an academic paper in English entitled "The Snuffle Encryption System," and in "source code" written in "C", a high-level computer programming language, detailing both the encryption and decryption, which he calls "Snuffle.c" and "Unsnuffle.c", respectively. Once source code is converted into "object code," a binary system of a series of Os and is read by a computer, the computer is capable of encrypting and decrypting data. In other words, the first program converts readable material into a code that could be only read by using the second program. As a consequence, his system has great promise to accommodate the four major uses of cryptography.

Snuffles" Snuffed By The Government

In 1992 Bernstein submitted a commodity jurisdiction request to the State Department about Snuffle.c and Unsnuffle.c (together referred to as Snuffle 5.0), and his other academic writings describing the Snuffle system. The State Department considered Bernstein's request under the International Traffic and Arms Regulations (ITAR) to discuss his snuffle system, the snuffle files, and his academic paper describing

the snuffle system at academic meetings and conferences. The Department determined that the commodity Snuffle 5.0 was a defense article on the munitions list and subject to licensing by the Department of State prior to export.

Bernstein Seeks Relief From Restraint of Free Speech

Alleging that he was not free to teach, publish, or discuss with other scientists his theories on cryptographic knowledge expressed in his snuffle program, Bernstein brought an action challenging the constitutionality of the International Traffic and Arms Regulation as violation his rights of speech and expression under the First Amendment of the U.S. Constitution. In *Bernstein 1*, 945 F. Supp. 1426 (N.D. Cal. 1996), the District Court found that the source code was expressive speech for the purpose of the First Amendment and plaintiff's claims presented a legitimate constitutional challenge and was accordingly justifiable. In *Bernstein 2*, 945 F. Supp. 1279 (N.D. Cal. 1996), the Court concluded that the licensing requirement for encryption software under the ITAR constituted an unlawful prior restraint of Professor Bernstein's freedom of expression. The court issued its decision in *Bernstein 2* on December 9, 1996.

The President Transfers Jurisdiction

Days before the decision in *Bernstein 2*, President Clinton issued Executive Order 13026, titled "Administration of Export Controls on Encryption Products." In the executive order he directed that the jurisdiction over non-military encryption products and related technology be transferred from the Department of State to the Department of Commerce. The executive order indicated, "the export of encryption software, like the export of other encryption products in this section, must be controlled because of such software's *functional* capacity rather than because of any possible *informational* value of such software." That language was apparently chosen by government lawyers familiar with the pending Bernstein case to cleverly characterize encryption technology as functional (mechanical) engines

that only drove the programs rather than speech or expression of ideas. Shortly thereafter, on December 30, 1996, the Department of Commerce issued an interim rule to allow jurisdiction over, and impose new combined national security and foreign policy controls on, certain encryption items. The regulations define export as "an actual shipment or transmission of items subject to the EAR out of the United States, or release of technology or software subject to the EAR to a foreign national in the United States [61 Fed. Reg. 68572 (Dec. 30, 1996)]. The President's Executive Order, and the resulting Commerce regulations, were viewed by Bernstein as a thinly disguised attempt to circumvent the court's ruling in *Bernstein 2*.

Exceptions Do Not Apply

A number of export licensing exceptions are available under the EAR. However, as directed by the President and implemented by the new regulations, these exceptions do not apply to encryption commodities or software. In addition, the EAR allows for broadly defined exceptions from the regulations for information resulting from fundamental research and educational information developed by scholars and scientists. Again neither of these exceptions applies to the development of encryption software. Finally, while an applicant who is denied a license is informed of appeal procedures, the EAR does not appear to allow for a judicial review.

Encryption Technology is Subject to Regulation

The President, and Department of Commerce, alleged that the President's authority to issue regulations controlling the dissemination or export or encryption technology flows from the International Emergency Economic Powers Act (IEEPA) [50 U.S.C. Section 1701-1706]. The Act authorizes the President to "deal with any unusual and extraordinary occurrence which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States, if the President declares a national emergency with re-

spect to such threat." Under this authority the President may "investigate, regulate, or prohibit any transaction in foreign exchange, and investigate, regulate, direct and compel, nullify, void, prevent or prohibit any exportation of any property in which any foreign country or foreign national thereof has any interest." The government said that exempting encryption software on the basis that it is protected under the First Amendment would be to impose a novel theory of free speech not contemplated by Congress.

Unfortunately, for the government, the legislative history in the House Conference Report, contradicts the government's position because it reveals that the House intended to protect First Amendment rights by insuring that "that no embargo (under IEEPA) may prohibit or restrict directly or indirectly the import or export of information that is protected under the First Amendment in the U.S. Constitution." Apparently, the language was explicitly intended, by including the words "directly or indirectly" to have a broad scope.

The court did find, however, that the regulation of encryption items is not totally prohibited and therefore does not exceed the statutory authority provided by the IEEPA. The court recognized that while the authority to regulate encryption technology may exist, it nonetheless must be accomplished within the bounds of the First Amendment.

The Applicable First Amendment Bounds

As the Supreme Court has often stated, in determining the bounds of the speech and expression guarantees of the First Amendment, "it has been generally, if not universally, considered that it is the chief purpose of the guarantee to prevent previous restraints upon publication," *Near v. Minnesota*, 283 U.S. 697 (1931). It is for this reason that the Court has held: "Any prior restraint on expression comes to this Court with a 'heavy presumption' against its constitutional validity," *Austin v. Keefe*, 402 U.S. 415 (1971). The thread running through numerous court cases is that prior restraints on speech and

publication are the most serious and the least tolerable infringement on First Amendment rights. A prior restraint has an immediate and irreversible sanction. If it can be said that a threat of criminal or civil sanction after publication "chills" speech, prior restraint "freezes" it at least for the time, *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539 (1976).

Self-Censorship a Danger

Interference with protected speech and Self-censorship is a danger because by the very terms of the encryption regulations, the most common expressive activities of scholars--teaching a class, publishing their ideas, speaking at conferences, or writing to colleagues over the Internet--are subject to a prior restraint by the export controls when they involve cryptographic source code or computer programs. In the field of applied science ideas are not just expressed in abstract, theoretical terms, but in precise applications. Those applications are subject to licensing under the encryption regulations and are specifically excluded from the exemptions for fundamental research and educational information. This is precisely the kind of law that encourages self-censorship on the part of those that must apply for licenses and unwarranted censorship on the part of the decision maker. As the American Association for the Advancement of Science (AAAS) stated to the Commerce Department in their comments regarding the new regulations, the "basic thrust" of the Interim Rule threatens to undermine essential features of scientific freedom and the open exchange of information that are generally acknowledged as critical to innovation in science and technology and are responsible in large part for the preeminence of America's research and development enterprise. AAAS has consistently opposed attempts by the government to restrict the communication or publication of classified research and technical information, efforts which they believe are inconsistent with scientific advancement.

Printed Material Exception Irrational

In addition, an exception for printed

materials, as opposed to computer programs, while at first glance a concession to the speech interests involved, is so irrational and administratively unreliable that it may well serve to only exacerbate the potential for self-censorship. As the AAAS commented, while it may be acceptable under this provision to publish encryption material in a book and distribute it internationally without an export license, putting the same information on a disk and sending it abroad is subject to ITAR approval. This distinction has serious ramifications for scholarly communication as many professional journals are now moving onto the Internet as world-wide electronic publications.

The Supreme Court's recent decision in *Reno v. American Civil Liberties Union*, 117 S.Ct. 2239 (1997), suggests that not only is the distinction between print and electronic media increasingly untenable, but that the Internet is subject to the same exacting level of First Amendment scrutiny as print media. Thus, the court stated that the dramatically different treatment of the same materials depending on the medium by which they are conveyed, paper or computer program, is not only irrational, it may be impermissible under traditional First Amendment analysis.

Final Analysis

As the court said in *Bernstein 2*, the fact that the government attempts to regulate encryption in the interest of national security does not alone justify a prior restraint. The court decided that the encryption computer codes were both functional and expressive (speech). The judge recognized that a computer software program often is used by scientists for expressive rather than just mechanical function reasons. The judge said that the new regulations struck at the most expressive activities of scholars and scientists like teaching a class, publishing their ideas, speaking at academic and professional conferences, or communicating over the Internet. In the field of applied science and mathematics ideas are not expressed solely in written abstract terms, but also in precise applications like Pro-

fessor Bernstein's computer codes. Consequently, said the court, to apply the new regulations to Bernstein would be to undermine the open exchange of ideas necessary for research and discovery. The court said that for a licensing scheme to be constitutionally applied to individuals like Bernstein, 1) the licensor must make the licensing decision within a specific and reasonable period of time; 2) there must be prompt judicial review; and 3) the government must bear the burden of going to court to uphold a licensing denial, and 4) once in court has the burden of justifying the denial. The Court believed that new, hastily drafted, Commerce regulations, like the old ITAR, did not provide these protections and were woefully inadequate to protect the First Amendment speech and expression interests of individuals like Bernstein.

Relief Sought For Others

In addition to seeking declaratory relief, Bernstein also sought a permanent injunction barring nationwide application of the encryption regulations on the grounds that loss of First Amendment freedoms constitutes irreparable injury, and that he will not be afforded complete relief unless an injunction extends to students, colleagues and others, with whom he might wish to communicate, who are not before the court.

Holding

The court declared that the Export Administration Regulations, 15 C.F.R. Part 730 et seq. (1997) and all rules, policies and practices that apply to or require licensing for export of 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 and may not be applied to the plaintiff's publishing of such items, including scientific papers, algorithms or computer programs.

The government was permanently enjoined from doing or causing to be done the following acts: a) further and future enforcement, operation or execution of the statutes, regula-

tions, rules, policies and practices declared unconstitutional under this order, including criminal or civil prosecutions with respect to plaintiff or anyone who uses, discusses or publishes or seeks to use, discuss or publish plaintiffs encryption program and related materials described in the case; or b) threatening, detaining, prosecuting, discouraging or otherwise interfering with plaintiff or any other person described in the court ruling.

Appeal

The government immediately requested a stay of the court's injunction order pending an appeal. It is reported that the judge will grant the stay request as it affects persons other than Professor Bernstein. He apparently will be allowed to distribute his "Snuffle" program.

Conclusion

The decision in this case in an admirable balancing of the security interests of the government with the scholar and scientist's First Amendment freedoms of expression and speech. The holding recognizes the government's interest in legitimate national security cases but requires the government to meet a high standard of proof and provides for a meaningful appeal process. The case draws a roadmap for the government to follow in cases where the national security is really at risk. Given the Clinton administrations fondness for government regulation we may expect revised regulations, based on this case, in the near future. This case, if affirmed on appeal, will surely lead to a desirable increased confidence in the security of electronic commerce. Surely increased security will cause the flower of electronic commerce to bloom.

Implications For Future Research

The Bernstein case highlights the conflict between the developers of encryption technology and government agencies. The developers believe that strong government regulation will result in the development of strong encryption programs overseas. Future research will focus on

legislative reaction to the Bernstein case and innovative ways that can be used by developers to comply with foreign and domestic market demands for strong encryption devices while accommodating legitimate law enforcement concerns. For example, some developers are proposing that they be allowed to maintain custody of their own keys that could be made available to the government when a court finds national security concerns so warrant.