First and Fifth Amendment Challenges to Export Controls on Encryption: Bernstein and Karn

Laura M. Pilkington

Follow this and additional works at: http://digitalcommons.law.scu.edu/lawreview

Part of the Law Commons

Recommended Citation
Laura M. Pilkington, Comment, First and Fifth Amendment Challenges to Export Controls on Encryption: Bernstein and Karn, 37 Santa Clara L. Rev. 159 (1996).
Available at: http://digitalcommons.law.scu.edu/lawreview/vol37/iss1/4

This Comment is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara Law Review by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.
FIRST AND FIFTH AMENDMENT CHALLENGES TO EXPORT CONTROLS ON ENCRYPTION: BERNSTEIN AND KARN

I. INTRODUCTION

The federal government encourages the expansion of the Internet and hails it as a revolution in the dissemination of information and as an avenue for commerce. However, the government uses its export control laws to restrict the exportation and dissemination of encryption software, a technology which is crucial to the expansion of the Internet and to the National Information Infrastructure, more popularly known as Vice President Gore's Information Superhighway. In defense of its export controls on encryption, the government cites national security and law enforcement concerns.

Software manufacturers complain that United States export controls prevent them from offering products that are readily available abroad, putting American firms at a serious competitive disadvantage with overseas software firms.

1. See The National Information Infrastructure: Agenda for Action (1993). With this document, the federal government announced its policy on the Internet and other networks which will make up the National Information Infrastructure (NII). The policy consists of nine principles which include (a) promoting private sector investment to expand competition, spur economic growth and create new businesses which benefit the American consumer, (b) promoting seamless, interactive, user-driven operation of the NII to enhance openness in communications and (c) to ensure information security and network reliability. Id. The last principle includes an action item to review United States policy on encryption technology. Id.


4. See infra notes 41-44 and accompanying text.

Civil libertarians charge that the export provisions restrict domestic communications on public cryptography, violating the First Amendment. For over five years, the federal government has been locked in a policy stalemate over its export controls on encryption, and Congress has introduced legislation to loosen controls several times, to no avail.

In an effort to understand the contradictory export control policy and the current debate, this comment examines the struggle occurring between the federal government, software manufacturers, and civil libertarians over this critical technology. After a discussion of the importance of encryption technology and how it works, Part II reviews the regulatory process for encryption exports. The remainder of Part II and Part III introduces the constitutional debate surrounding the export laws.

The comment concludes in Part IV that although the government has amended the regulations in response to pressure from business groups, its method of providing very narrow exceptions to an overly broad regulation has not succeeded in resolving the constitutional problems. The Arms Export Control Act's (AECA) exemption from judicial review, albeit limited, and several International Traffic in Arms Regulation (ITAR) definitions unconstitutionally re-
strict cryptographic communications and leave the legislation open to attack on free speech and due process grounds. Part V augments the analysis in Part IV with a discussion of the impact of the December 1996 *Bernstein* decision and jurisdictional shift in export regulations.

Part V concludes that recent developments do not resolve the constitutional problems posed in Part IV. Part VI proposes that Congress enact comprehensive encryption control reform legislation which meets First Amendment strict scrutiny standards. If Congress fails to act, then courts hearing First and Fifth Amendment challenges should limit exemptions from judicial review and strike offending provisions in the export control laws to bring them into constitutional conformance. The challenge facing the federal government is finding a way to empower its signals intelligence and law enforcement agencies without destroying a major sector of the economy and without violating the constitutional rights of its citizens.

II. BACKGROUND

A. The National Debate

1. The Struggle over Encryption Technology

Encryption, the process of encoding and decoding information, has become an indispensable technology for protecting information of all kinds from unauthorized disclosure. With the tremendous growth of telecommunications and computer technologies over the past two decades, cryptography, which has been around for centuries, is now routinely required and used by businesses in mass-marketed applications software.

Data encryption is currently employed in networking, word processing, e-mail, and many other communication

12. See discussion *infra* part IV.B.
13. See discussion *infra* part V. The analysis in Part IV was current as of November 1996. Part V, the Recent Developments section, is appended to reflect changes occurring in December of 1996 and to show how these events modify the analysis in Part IV.
14. See discussion *infra* part V.C.
15. See discussion *infra* part VI.A.
16. See discussion *infra* part VI.B.
17. See *Cryptography (from Julius Caesar Through Public Key Cryptosystems)*, *in Building in Big Brother*, *supra* note 6, at 7.
products.\textsuperscript{19} It ensures the security of electronic funds transfers and is used extensively in wireless communications.\textsuperscript{20} Because it permits secure transactions on a relatively unsecure worldwide computer network, this technology is seen as essential to the commercial expansion of the Internet.\textsuperscript{21}

Because early use of cryptography was primarily for intelligence gathering and securing military communications, the Defense Department, through the National Security Agency (NSA) has played a key role, both in the development of the science and in the control of its use in the United States and abroad.\textsuperscript{22} The NSA views the spread of cryptography as a threat to national security and has continued efforts, begun just after World War II, to control the development and expansion of cryptography in the private sector.\textsuperscript{23} The government contends that "[t]he uncontrolled availability abroad of cryptographic devices and software would hinder the United States' ability to gather foreign intelligence on national security and foreign policy matters."\textsuperscript{24}

In addition to export controls, the government has tried to slow the growth and dissemination of cryptography through control of public funding for cryptography, patent publications, and the dissemination of scientific papers at academic conferences.\textsuperscript{25} In 1975, the NSA tried to stop all National Science Foundation (NSF) grants for cryptology research.\textsuperscript{26} The two agencies agreed on coordinated funding and review procedures which now allow the NSA to review all

\begin{itemize}
\item \textsuperscript{19} Microsoft Windows NT, Novell Netware, FileApps by HDC Corporation, and Lotus Notes are a few examples of business applications software using data encryption.
\item \textsuperscript{21} See supra note 3 and accompanying text.
\item \textsuperscript{22} Kenneth J. Pierce,\textit{ Public Cryptography, Arms Export Controls, and the First Amendment: A Need for Legislation, 17 Cornell Int'l L.J. 197, 202 (1984).}
\item \textsuperscript{23} Id.
\item \textsuperscript{25} Pierce, supra note 22, at 203. Pierce has a good discussion of the history of NSA attempts to control dissemination of cryptography in these areas. See also Susan Landau et al., Association for Computing Machinery,\textit{ Cryptography in Public: A Brief History, in Building in Big Brother supra note 6, at 43.}
\item \textsuperscript{26} Pierce, supra note 22, at 203.
\end{itemize}
applications pertaining to cryptography and gives the agency control of the funding decisions.\textsuperscript{27}

The NSA attempted to control private patent publications and the presentation of papers on cryptography at academic conferences.\textsuperscript{28} Each attempt was met with public criticism from the academic community, resulting in the NSA withdrawing from its extreme position.\textsuperscript{29}

However, the export control regime, which for cryptographic exports consists of the Arms Export Control Act (AECA)\textsuperscript{30} and the Export Administration Act (EAA),\textsuperscript{31} is still in place. These statutes and their implementing regulations continue to control the exportation of strong encryption\textsuperscript{32} and represent the last remaining controls the government has at its disposal to control the spread of public cryptography.\textsuperscript{33}

\section{2. United States Policy on Encryption Controls}

There is widespread agreement that the export controls on encryption hamper United States competitiveness\textsuperscript{34} and cause United States firms to lose worldwide market share for

\begin{quote}
\begin{itemize}
\item \textsuperscript{27} Id. at 203-04.
\item \textsuperscript{28} Id. at 204.
\item \textsuperscript{29} Id.
\item \textsuperscript{32} The term "strong encryption" refers to systems that are reasonably secure, such that the time, effort, and money required to break the system is greater than what the data is worth to most people, thereby making the effort to break the system futile. See BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY (John Wiley & Sons, 2d ed., 1996) for a more thorough discussion of encryption strength.
\item \textsuperscript{33} Although technically the State Department through the Office of Defense Trade Controls (ODTC) has control of the administration of exports with encryption under the AECA, this office must seek the Defense Department's (NSA's) concurrence with its decisions. See U.S. GEN. ACCOUNTING OFFICE, GAO/NSIAD-93-67, EXPORT CONTROLS: ISSUES IN REMOVING MILITARILY SENSITIVE ITEMS FROM THE MUNITIONS LIST, 11-21 (1993) [hereinafter Removing Militarily Sensitive Items]. In one instance, the State Department attempted to transfer export administration of mass market software to Commerce Department jurisdiction because it did not believe it was possible to control such software. Id. at 20. The NSA refused to allow the transfer, citing Commerce Department controls as inadequate and fears that such a move would lead to decontrol of encryption. Id. at 21. The NSA prevailed in the dispute and encryption software remained under State Department jurisdiction. Id.
\item \textsuperscript{34} The competitiveness of the software industry is not the focus of this comment. However, the impact of business groups must be examined to understand the development of export control laws as applied to encryption, since the
\end{itemize}
\end{quote}
mass marketed software, an industry which United States firms previously dominated.35

In January of 1996, the Clinton Administration acknowledged this predicament and expressed some willingness to ease controls.36 Then Secretary of the Commerce, Ron Brown, admitted that "[i]f your foreign competitors are exporting products with encryption capability and you are not, that puts you at a tremendous competitive disadvantage."37

The Administration's admission stemmed from a joint study by the NSA and the Commerce Department on the effect of export controls on United States competitiveness.38 This study concluded what business groups and scholars have been arguing for several years: Encryption controls are harming United States firms.39 United States companies stand to lose as much as thirty percent of the $200 billion in United States computer system sales expected in the year 2000 because of these export restrictions on encryption.40

The NSA, however, relies heavily on the limited availability and use of cryptography to carry out its functions.41 The agency is responsible for ensuring that government communications and data are secure, and that the United States is able to intercept and decipher the codes of other countries.42 Most people would agree that keeping government communications secure and intercepting the transmissions of foreign countries are critical to an effective foreign policy and national security.43 In fact, many in Congress consider the


37. Id.

38. Id.

39. Id.; see also sources cited supra note 35 (for a discussion on the harm to United States competitiveness).

40. Scrambled Software Gets an OK, supra note 36, at 1D.


42. Pierce, supra note 22, at 201.

43. In addition, the Federal Bureau of Investigation (FBI) has argued that widespread availability of strong encryption makes it difficult if not impossible for government agencies to effectively use wiretaps against criminals, drug dealers, and terrorists. If law enforcement becomes ineffective as a result of the
NSA to be the "single most important source of intelligence for the nation." 44

3. The Effectiveness of the Controls

What is problematic is the plausibility of the government's stated policy reasons for restricting public cryptography exports, given the availability of strong cryptography outside the United States. 45 The government contends that the uncontrolled availability overseas of cryptographic devices and software impede the United States' ability to gather foreign intelligence on national security and foreign policy matters. 46 However, exports of software with encryption from the United States cannot reasonably be expected to substantially affect the availability of strong encryption in other countries, since such products are widely available in so many countries. 47 A recent study conducted by the Software Publishers Association found cryptographic products equivalent or better than United States products to be distributed by at least 340 companies in 22 countries. 48 The NSA refuses to make public its additional reasons for its actions regarding cryptography. 49 They are considered classified. 50

It is more likely that the government is trying to control public cryptography in the United States because of its potential to create new encryption systems that its agencies cannot break, or at least, in which U.S. agencies must invest sub-

---

44. Pierce, supra note 22, at 202 (quote by Senator Walter Mondale on the role played by the NSA).
46. See supra note 24 and accompanying text.
47. See Testimony, supra note 45, at 478-79.
48. Id. at 478.
49. See Evans, supra note 35, at 492.
50. Removing Militarily Sensitive Items, supra note 33, at 21.
stantial time and resources to break. The government, thus, has a significant interest in making sure that no strong cryptography is developed which is not under its control.

Because the NSA was once the dominant producer of more advanced cryptography — possibly worldwide — and still possesses much of the expertise in this area, this agency in particular has a strong interest in maintaining the status quo. The development of public cryptography may expose weaknesses in the systems used by the NSA, on which it must rely to do its intelligence work. This might happen, for example, because advances in the science reveal certain features in the systems employed by United States defense agencies which other countries may then exploit.

Advances in the science may also alert other nations to the vulnerabilities in their own systems, or to the NSA’s ability to decipher the systems employed by other nations. Thus, they would change their encryption systems and the NSA would be faced with having to crack new, advanced systems. Whatever the reason, concerns about U.S. encryption policy focus on the NSA’s attempts to slow the growth and dissemination of cryptographic devices both abroad and within the United States.

4. The Constitutional Problem: The First and Fifth Amendments

If, in fact, the government is using export laws to control the dissemination of strong cryptography not only abroad, but also within the United States, then it is effectively applying regulations designed for national security administration to achieve control over the domestic development of cryptography. This situation poses serious First and Fifth Amend-

51. SCHNEIER, supra note 32, at 597-98.
52. Id. at 598.
53. Id. at 597-98.
54. See Bamford, supra note 41.
55. See SCHNEIER, supra note 32, at 597-98.
56. Id.
57. See Testimony, supra note 45, at 487; see also Evans, supra note 35, at 480.
ment concerns. At the very least, it can be argued that the administration has exceeded its statutory authority.

In defining terms for the control of exports overbroadly, so as to include cryptographic communications, and in requiring a license prior to publication, the government arguably imposes a prior restraint on publication, thereby violating the First Amendment. In addition, because the export control statutes do not allow for judicial review of the agency's determination and do not allow one to appeal except to the director of the overseeing agency, they may also violate Fifth Amendment due process rights.

It is not only civil libertarians that have voiced many of these concerns. The United States Justice Department's Office of Legal Counsel has concluded on three different occasions that the AECA and ITAR, as applied to cryptography are likely unconstitutional. It is their opinion that the export control statutes and regulations can be applied unconstitutionally to regulate speech and the licensing scheme may operate as a prior restraint.

B. Understanding Encryption

In order to follow the debate surrounding the export control laws as they apply to cryptography, it is necessary to discuss how encryption works to secure electronic communications and the specifics of the regulations.

1. Encryption Basics

If a sender wants to send a secure message to a receiver, the sender can encrypt the message to disguise its sub-
The undisguised message is called plaintext or cleartext, and the encrypted message is known as ciphertext. The process of turning ciphertext back into the original plaintext is decryption.

A cryptographic algorithm, also called a cipher, is a mathematical function used for encryption and decryption. There are usually two related functions to an algorithm, one for encryption and the other for decryption. "The art and science of keeping messages secure is cryptography, and it is practiced by cryptographers. Cryptanalysts are practitioners of cryptanalysis, the art and science of breaking cipher text."

The security of early algorithms was dependent on the users' ability to keep secret the way the algorithm works. Modern cryptography has solved this problem by using a key (or keys). Keys are inversely related, such that what one does, the other can undo. What needs to be kept secret in modern cryptography is the key, not the algorithm itself. This allows the algorithm to be published and analyzed by its potential users. Also, the fact that the algorithm is freely available means that products with the algorithm are more easily mass produced. As long as people do not have your key, they cannot decrypt your messages, even though they have the encryption algorithm.

a. Single Key Systems

There are two types of modern (key-based) algorithms. The first type is the symmetric algorithm, also called private
key or single key cryptography. A single key is used both to encrypt and to decrypt the message. A separate key is needed for each pair of users who exchange messages, and both sides must keep the key a secret to keep the system secure.

The Data Encryption Standard (DES) algorithm is an example of a private key system. The main problem with this type of system is key exchange. In order for the system to work, a pair of users must exchange keys and keep them secret, which requires a reliable method for distributing the keys. Key exchange is a potential breach of security in the system because more than one person must be trusted with a confidential key, and because the key could be discovered during an exchange.

b. Asymmetric Key Systems

The second type of encryption algorithm was devised to solve the key exchange problem. This algorithm is an asymmetric key system or public key cryptography, which uses two keys, a public key and a private key for each individual user. A user must keep his or her private key secret, but the user’s public key may be published freely. In fact, the public keys can be listed in a directory of electronic mail addresses, similar to a phone book.

An individual’s public and private keys are mathematically related, such that if a sender encrypts a message with the receiver’s public key, only the receiver can decrypt it with his or her private key. The sender does not have to know the receiver’s private key to encrypt the message. Because only the receiver’s private key can decrypt the message, the

79. Id.
80. Id.
81. Id.
82. Id.
83. Rubenstein, supra note 20, at 183.
84. Id.
85. Id.
86. RSA and PGP (Pretty Good Privacy) are examples of public key systems.
88. Id.
89. Id.
90. Id.
91. See Rubenstein, supra note 20, at 184.
sender knows that only the intended receiver is getting the message.\textsuperscript{92} The only way to break security in the public key system\textsuperscript{93} is by giving away your private key.\textsuperscript{94} This is far less likely to happen, since no private key exchange is necessary for the system to function.\textsuperscript{95}

2. Encryption Keeps Communications Secure

The security of an encryption system is directly related to the length of its key (or keys).\textsuperscript{96} The longer the key length, the larger the number of possible combinations. Thus, as the key length is increased, it takes more time (or more computing power) for a cryptanalyst to uncover the key, and the system is more secure.

The two most widely used systems are DES and RSA.\textsuperscript{97} The symmetric key DES system has a fixed key length of 56 bits.\textsuperscript{98} International Business Machines (IBM) developed DES in conjunction with the NSA, and it is an approved government standard.\textsuperscript{99} The details of the algorithm are freely available from the National Institute of Standards and Technology (NIST).\textsuperscript{100} DES is readily available overseas, yet the ODTC does not allow its export from the United States except in two very limited circumstances.\textsuperscript{101} DES is widely used by banks and other financial institutions for their electronic communications, including electronic funds transfers.\textsuperscript{102}

\textsuperscript{92} Id. at 183-84.

\textsuperscript{93} Security in a public key system is a function of the difficulty of deriving the private key from the public key. Id. at 183-84. The inverse mathematical relationship between the two keys makes this very difficult. Id. Because so much computing power is needed for this task, the security of the system is enhanced. \textit{See generally} Schneier, \textit{supra} note 32, at 8 (discussing computing power and security).

\textsuperscript{94} This is an oversimplification in that there is an esoteric problem of corruption of public keys. However, compared to the potential security breach inherent in symmetric key systems, this is a minor problem. \textit{See} Schneier, \textit{supra} note 32, at 8, for an in-depth discussion of algorithm security.

\textsuperscript{95} Id.

\textsuperscript{96} \textit{Computer Security Basics, supra} note 67, at 19.

\textsuperscript{97} Id.

\textsuperscript{98} See Rubenstein, \textit{supra} note 20, at 184, for a discussion of what is currently used today. \textit{See also} notes 106-08 \textit{infra} and accompanying text.

\textsuperscript{99} Id.

\textsuperscript{100} Id. at 185.

\textsuperscript{101} The exceptions are if it is used by a financial institution for securing financial transactions or by subsidiaries owned at least 51\% by United States corporations. \textit{See} Id. at 185-86.

\textsuperscript{102} Rubenstein, \textit{supra} note 20, at 182.
The privately developed asymmetric key RSA system has variable length keys. It was developed by three mathematicians (Ronald Rivest, Adi Shamir and Leonard Adelman), after whom it is named. RC2 and RC4 are two additional asymmetric encryption algorithms designed by Ron Rivest, which also have variable key lengths, and when used with longer key lengths are considered good alternatives to DES. Public key, or asymmetric systems, require much longer key lengths than symmetric systems to maintain an equivalent security level. As will be discussed, the AECA and ITAR regime restricts the exportation of all products using DES, as well as those products using RSA which have a key length over 40 bits. Many cryptographers believe that the encryption currently allowed under export controls is inadequate.

The implications of these technologies should be emphasized. Particularly with public key encryption, where no prearranged trust relationship is required between parties to obtain secure communications, the benefits of the technology is immediately apparent. The ability to publish one's public key along with one's electronic mail address, allows for widespread and regular use of the system for secure and private

<table>
<thead>
<tr>
<th>Symmetric Key Length</th>
<th>Public-key Key Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>56 bits</td>
<td>384 bits</td>
</tr>
<tr>
<td>64 bits</td>
<td>512 bits</td>
</tr>
<tr>
<td>80 bits</td>
<td>768 bits</td>
</tr>
<tr>
<td>112 bits</td>
<td>1792 bits</td>
</tr>
<tr>
<td>128 bits</td>
<td>2304 bits</td>
</tr>
</tbody>
</table>

*Id. at 166, tbl. 7.9.*

103. *Id.* at 185.
104. *Id.*
105. *Id.* at 186.
106. There are a number of technical reasons for this which are well explained in Schneier, supra note 32, at Chapter 7. The following table shows that public key systems such as RSA need a much longer key length to get the equivalent security protection.

107. See infra part II.B.3 for a discussion of ITAR restrictions and part V for an update and analysis of the December 1996 amendments to the export laws under Executive Order 13026.

Ensuring security and privacy in one's communications, both domestic and international, by utilizing a strong encryption system, is seen as essential to the expansion of the Internet and other networks, as media for both political discourse and commerce.\textsuperscript{110}

3. The Regulation of Cryptographic Exports\textsuperscript{111}

The U.S. export control of cryptographic exports actually consists of two schemes. A stricter one for "munitions" is governed by the Arms Export Control Act\textsuperscript{112} (AECA), and a generally more lenient scheme for "dual-use" items, which have both civilian and military purpose, comes under the Export Administration Act\textsuperscript{113} (EAA).

a. State Department and NSA Control of Encryption Exports Through the USML and Licensing

The State Department exercises authority over the United States Munitions List (USML), which was created under the authority of the AECA and is administered through the ITAR.\textsuperscript{114} Requests to license items listed on the USML are made through the Office for Defense Trade Controls (ODTC) in the State Department, and regulatory decisions are made with the concurrence of the Department of Defense, through the NSA.\textsuperscript{115} The Department of Commerce, through its Bureau of Export Administration (BXA), makes licensing decisions for the Commerce Control List (CCL), created under the EAA and the implementing Export Administration Regulations (EAR).\textsuperscript{116}

Under penalty of criminal sanction, once an item is placed on the USML or on the CCL, it may not be exported without first obtaining an export license from the respective

\textsuperscript{109} Computer Security Basics, supra note 67, at 19.
\textsuperscript{110} See supra note 3 and accompanying text.
\textsuperscript{111} See supra note 3 and accompanying text.
\textsuperscript{112} See discussion supra part V for an update and analysis of the December 1996 amendments to the regulation of cryptographic exports.
\textsuperscript{115} 22 C.F.R. §§ 120-30 (1994).
\textsuperscript{116} Removing Militarily Sensitive Items, supra note 33, at 10-11.
Secretary. The maximum penalty for violating AECA is $1,000,000 and/or imprisonment for not more than ten years, and the maximum penalty for an EAA violation is five times the value of the exports or $1,000,000, whichever is greater, and/or not more than 10 years imprisonment.

The legislative purpose for controlling munitions, as stated in the AECA policy provision, is to further "world peace and the security and foreign policy of the United States." The EAA purpose statement is much broader, containing fifteen separate policy statements which include the goals of regulating to restrict exports that increase the military potential of other countries, controlling domestic short supply, and ensuring American competitiveness in international markets.

b. Encryption Is a "Munition" Subject to Determination and Licensing Processes

The export control scheme considers data encryption a "munition" or predominantly military in application, and therefore views the regulations as necessary to safeguard the national security of the United States. The ODTC has primary jurisdiction over cryptographic software because it is listed as a "munition" under Category XIII(b)(1) of the USML.

To determine whether an item one wants to export is on the USML, one must submit to the ODTC a Commodity Jurisdiction application (CJ). The ODTC then makes an individual determination as to whether a person's item is subject to State Department jurisdiction. Persons wishing to export items within State Department jurisdiction must register as an arms dealer with the ODTC and apply for an indi-

117. Id. at 11-12.
119. 50 U.S.C. app. § 2410(b) (Supp. 1996). In the case of an individual, the fine is not more than $250,000, instead of $1,000,000. Id.
123. Removing Militarily Sensitive Items, supra note 33, at 11.
124. Id.
125. See generally, Rubenstein, supra note 20, at 186-98, for a complete overview of the CJ process.
In contrast to the AECA scheme, the EAA provides for general licenses for software and technology that is "publicly available" and for mass marketed software, permitting the exporter to classify the items themselves and export without BXA processing an application.

c. Extent of Control Over Encryption Export

Originally, Category XIII(b)(1) of ITAR included all cryptographic systems. However, software manufacturing industry opposition resulted in a 1992 compromise by the government. Certain limited items are now allowed "automatic" transfer to Commerce Department jurisdiction, administered by the BXA. These items are:

1. decryption only for copy-protected software;
2. bank or money transactions;
3. cryptographic processing using analogue techniques in certain radio and fax equipment;
4. certain personalized "smart" cards;
5. access control devices such as ATMs;
6. data authentication;
7. fixed data compression or coding techniques;
8. set top decoders; and
9. anti-virus software.

Items which perform these and no other functions are automatically transferred to BXA control and will generally

126. Id. at 199. An individually validated license requires an exporter to apply for a separate license for each end user. There are no general licenses under ITAR. Id.
127. Publicly available software includes items (1) sold from stock at retail selling points, (2) available in over the counter transactions and (3) designed for installation by the user without support from the supplier. Larry E. Christensen, Technology and Software Controls Including Recent Changes in Country Scope, in COPING WITH U.S. EXPORT CONTROL 1994, at 161 (PLI Commercial Law & Practice Course Handbook Series No. A-705).
128. See id. at 153-62. These less restrictive export controls are available to persons exporting to most countries. However, more stringent controls are placed on those exporting to certain countries deemed a threat to national security, such as Iran or Libya. Id.
129. Rubenstein, supra note 20, at 187.
130. For procedures resulting from this compromise see id. at 195-96. For the most recent (December 1996) changes to the regulations see part V.B.
be classified under information securities in Category 5 of the CCL. 133 This regime offers much less restrictive licensing controls and shorter processing times. 134 If the software performs any other encryption functions than those listed in (1)-(9), however, it continues to be subject to ITAR. 135 The compromise also established expedited transfers of mass-marketed software if the software uses the RC2 or RC4 algorithm and has a key length less than 40 bits. 136 This expedited transfer authority is referred to as the SPA Agreement. 137

All items not meeting these characteristics for expedited processing are subject to case-by-case review by the ODTC. 138 Most industry analysts agree that while the compromise makes an attempt at expedited processing and an easing of restrictions, the current controls are still too restrictive to be useful for most exporters of mass-marketed software. 139 Further, algorithms that are not mass-marketed presumably would not qualify for the less onerous controls if they did not fall into categories (1)-(9) above.

The AECA and EAA, as interpreted by the administering agencies, also differ significantly in the ability to appeal decisions and the availability of judicial review. While appeal and judicial review of agency decisions under the EAA are limited by a statutory preclusion from the APA, this scheme contains well defined procedures for bringing claims to court and definitive time limits for agency action. 140 Under the

133. Rubenstein, supra note 20, at 195.
134. See Removing Militarily Sensitive Items, supra note 33, at 12.
135. Rubenstein, supra note 20, at 195.
136. Id. at 195-96.
137. SPA stands for the agreement the Bush Administration reached with the Software Publishers Association, a business group of software manufacturers.
138. Rubenstein, supra note 20, at 197.
139. Robert Holleyman, Pres., Business Software Alliance, On the Export of Software with Encryption Capabilities, Testimony at the National Institute of Standards and Technology (Sept. 6, 1995) (on file with author) [hereinafter Holleyman Testimony].
140. See John Elicott, et al., Judicial Review Under Export Laws, in COPING WITH U.S. EXPORT CONTROLS 1994, at 357-62 (PLI Commercial Law & Practice Course Handbook Series No. A-705). The procedures include the ability to appeal civil enforcement actions to an administrative law judge (ALJ), review of the ALJ decision by the Secretary of Commerce, and appeal of the Secretary's decision to the U.S. Court of Appeals for the District of Columbia Circuit. Id. at 357-59. For penalty determinations brought by the BXA, an exporter may be heard in a federal district court, which is empowered to determine de novo all issues necessary to the establishment of liability. Id. at 359-60.
ODTC's interpretation of the AECA, the CJ process allows only for appeals within the executive branch of government\(^{141}\) and there are no time limits within which the agency must act in rendering a final decision.\(^{142}\)

C. Constitutional Challenges

The current export regime on encryption raises several First Amendment issues. First, government regulations are potentially being used not just to prevent exports, but to stifle communication about encryption, in that the regulations prohibit an individual from publishing information in any way that would make it available to a foreign national.\(^{143}\) Since this covers almost any dissemination of cryptographic communications, it is a potential violation of First Amendment protection for political, commercial and scientific speech.\(^{144}\)

Civil libertarians also argue that encryption makes privacy in speech possible for electronic communications, and thus should enjoy special protection under the First Amendment.\(^{145}\) Cryptography functions like an "envelope" for administrative claims by an exporter, the EAA allows for a limited action in federal district court to compel the agency to act on an application. \(\text{Id.}\) at 361-62.

141. The appeals process can be described as follows:

   Appeals can be made from an initial CJ determination at the Office of Defense Trade Control to the Director of the Center for Defense Trade, who must reply within 30 days. If the decision at the Center for Defense Trade is unsatisfactory, a further appeal can be lodged with the Assistant Secretary for International Politico-Military Affairs, who does not have a time limit for reply.


142. \(\text{See 22 C.F.R. § 126.7 (1993).}\)

143. \(\text{See discussion infra part IV.A.}\)

144. \(\text{See Shinn, supra note 60, at 379. See also United States v. Edler, 579 F. 2d 516 (9th Cir. 1978). Although litigated under a precursor statute to the AECA, this case is one of the few making a First Amendment challenge to the export regime. In this case, an exporter of missile components was convicted of violating the Mutual Security Act of 1954 by exporting without a license and appealed on First Amendment and overbreadth grounds. Id. at 516-18. The court held that the statute as applied in the commercial speech context did not interfere with constitutionally protected speech. Id. at 519-21. Additionally, the court narrowly construed the technical data definition so that the exports had to be "significantly and directly related to specific articles on the Munitions List." Id. at 521. The court also mentioned in dicta that the effect on speech in such circumstances as Edler's might be considered incidental, in which case a less stringent First Amendment test is allowed, as given in United States v. O'Brien, 391 U.S. 367 (1968). Id. at 520.}\)

145. \(\text{See supra note 6, at 412.}\)
Electronic communications: Requiring people to send their electronic mail unencrypted is analogous to requiring people to use only postcards. When one knows that potentially anyone can read otherwise private communications, one will tend to communicate only that which is not private.

1. Bernstein v. United States: A Free Speech Challenge to AECA and ITAR

Because the AECA and ITAR, as enforced by the ODTC and NSA, potentially restrict cryptographic communication as well as exports of the technology, First Amendment challenges to the application of ITAR to encryption devices have been filed and are now being decided in federal courts. The first, Bernstein v. United States, was brought by a mathematics graduate student at the University of California at Berkeley, who developed an algorithm named “Snuffle” and wished to post it on the Internet for review by other cryptographers. He submitted a CJ application to the ODTC for three items: a paper on his algorithm and two source code files. In his application correspondence with the ODTC, Bernstein was informed that his “Snuffle” commodity was subject to AECA jurisdiction and would require him to register as an arms dealer and obtain a license.

Bernstein argues that this restriction effectively prohibits him not only from posting his cryptography on the Internet (which reaches beyond U.S. borders), but also from any publication, since dissemination in almost any form is likely to be disclosed to some foreign national in the United States.

---

146. The envelope analogy has become popular in the literature on encryption. See e.g., Rubenstein, supra note 20, at 183. This postcard example is taken from Plaintiff's Memorandum of Points and Authorities in Support of Motion for Partial Summary Judgment and/or Summary Adjudication of Issues at 15, Bernstein v. United States, 922 F. Supp. 1426 (N.D. Cal. 1996) (No. 95-00582).

147. Plaintiff's Memorandum at 15, Bernstein (No. 95-00582).


150. Bernstein has since received his doctorate and is teaching at the University of Illinois.


152. Id.
and, therefore, would meet the definition of an "export" under ITAR.\(^{153}\)

In addition to violations of the First Amendment, overbreadth and vagueness, Bernstein contends\(^{154}\) that the regulations fail to provide procedural safeguards against unbridled discretion and arbitrary and capricious action by regulators, thus, violating his due process rights.\(^{155}\) He asked the court to declare these provisions of ITAR and AECA unconstitutional and in violation of the Administrative Procedures Act\(^{156}\) (APA), and sought an injunction to restrain the ODTC from preventing publication.\(^{157}\)

Bernstein's claim survived a motion to dismiss by the government.\(^{158}\) The \textit{Bernstein} case has attracted a great deal of attention in the legal and mainstream press because the trial court concluded that Bernstein's source code is speech for purposes of the First Amendment.\(^{159}\) Essentially, this conclusion, and the denial of the motion to dismiss, cleared the way for a full consideration of the First and Fifth Amendment issues.

---

\(^{153}\) See discussion \textit{infra} part IV.A.1 (giving the ITAR definition for export).


\(^{155}\) To make these First and Fifth Amendment arguments, Bernstein relies on several important cases, all of which are discussed \textit{infra} in part IV.B-C. \textit{Freedman v. Maryland}, 380 U.S. 51 (1965), provides the plaintiff with a strenuous free speech test against licensing statutes which operate as prior restraints on expression. Here, the Supreme Court held unconstitutional sections of a Maryland statute which required motion picture exhibitors to submit films for prior approval and obtain a license. \textit{Id.} at 60. The Court held that before any restraint upon protected expression may become final, it must be subjected to prompt judicial review in a proceeding in which the government will bear the burden of justifying its decisions. \textit{Id.} at 58-59. In \textit{New York Times v. United States}, 403 U.S. 713 (1971), where the government sought to enjoin newspapers from publishing the contents of a classified historical study on United States policy in Vietnam, the Supreme Court held that "[a]ny system of prior restraints of expression comes to the Court bearing a heavy presumption against its constitutional validity." \textit{Id.} at 714. Finally, \textit{Near v. Minnesota ex rel. Olson}, 283 U.S. 697 (1931), holds that while prior restraints on speech are not unconstitutional per se, they are nearly so. \textit{Id.} at 700.


2. Karn v. United States: Encryption as a Functional Commodity

Another recently filed case was, *Karn v. United States,*\(^1\)\(^6\)\(^0\) which also makes First and Fifth Amendment challenges to the AECA and seeks to have provisions of ITAR declared unconstitutional and in violation of the APA.\(^1\)\(^6\)\(^1\) The controversy in this case concerns Philip Karn, a telecommunications engineer who has also developed several cryptographic algorithms.\(^1\)\(^6\)\(^2\)

Karn submitted two CJ applications to the ODTC for a determination. The first was for a published book containing a collection of algorithms\(^1\)\(^6\)\(^3\) and the second was for the same algorithms on a floppy disk.\(^1\)\(^6\)\(^4\) The ODTC determined that the book, which contained the algorithms in printed form, was not subject to its export jurisdiction because it was in the public domain.\(^1\)\(^6\)\(^5\) However, the information on the floppy disk (which was identical to that in printed form in the book) was nonetheless subject to its jurisdiction because it was in the form of source code and thus considered a functional commodity.\(^1\)\(^6\)\(^6\) Karn was therefore required to register as an arms dealer and obtain an export license for the material on the floppy, but he was able to freely export the book.\(^1\)\(^6\)\(^7\)

Even though it was the same information, the material on the floppy was considered technical information because it did not meet the definition for a public domain exception under ITAR.\(^1\)\(^6\)\(^8\) Karn appealed the ODTC's CJ decision on the floppy disk.\(^1\)\(^6\)\(^9\) Similar to Bernstein, Karn brought the


\(^{162}\) Rubenstein, *supra* note 20, at 205.

\(^{163}\) The book submitted was BRUCE SCHNEIER, *APPLIED CRYPTOGRAPHY* (John Wiley & Sons, 2d ed. 1996).


\(^{167}\) Rubenstein, *supra* note 20, at 205-06.

\(^{168}\) Plaintiff's Opposition at 7, *Karn* (95-01812).

challenge on First Amendment speech grounds, as well as Fifth Amendment due process grounds.\footnote{170}

In contrast to Bernstein's, Karn's challenge did not survive the government's motion to dismiss.\footnote{171} Relying on the political question doctrine, the court dismissed the APA claim as nonjusticiable and granted summary judgment to the government on the constitutional claims, stating that the issues posed by Karn were policy questions to be decided by the elected branches of government.\footnote{172} Karn's attorneys have filed a notice of appeal.\footnote{173}

Many people following the debate are perplexed by the different conclusions reached by the Bernstein and Karn courts.\footnote{174} Practitioners recognize that the decision handed down in Bernstein may be far reaching.\footnote{175} Bernstein and Karn are being watched closely not only by civil libertarians who want to protect privacy, but also by the business sector.\footnote{176} The business sector, of course, is concerned about the competitiveness of the U.S. software industry, which feels threatened by the export restrictions.\footnote{177}

But, there is more at stake for the commercial sector. A successful challenge to the export laws as applied to encryption could mean wider availability of high-quality encryption in software products overall.\footnote{178} Additionally, the ability to ensure security and privacy in one's communications, both

\footnote{170. Complaint at 2, Karn (95-01812).}
\footnote{172. Id. at 3.}
\footnote{173. The notice of appeal was filed on April 19, 1996.}
\footnote{174. David J. Loundy, Two Rulings on Encryption Speak Different Languages, CHI. DAILY LAW BULLETIN, May 9, 1996 at 6; A Tale of Two Crypto Court Cases: Are Karn and Bernstein Judges on the Same Planet?, INFORMATION LAW ALERT (May 3, 1996) <http://www.infolawalert.com>.}
\footnote{175. Edward J. Radlo, Legal Issues in Cryptography, COMPUTER LAW., May 1996, at 1, 8.}
\footnote{176. Holleyman Testimony, supra note 139.}
\footnote{177. See supra part II.A.2.}
\footnote{178. Software firms often complain that they have to develop separate programs for domestic and international markets; strong encryption for domestic products because people demand it in their software, and weak encryption for international sales because of the restrictions. See Holleyman Testimony, supra note 139. This dual development of products is costly to create and maintain and puts them at a significant competitive disadvantage. Id. at 2-4. Some firms avoid incorporating encryption into their software products altogether because they do not want to register as an arms dealer or have to become proficient at "munitions" exporting. See Hartzler, supra note 35.}
domestic and international, is essential to the expansion of the Internet both as a forum for political discourse and for commercial purposes.\textsuperscript{179}

\section*{III. Statement of the Problem}

By responding to business group pressures with incremental changes to the export laws, the government has failed to resolve the First and Fifth Amendment issues raised by the application of export controls to data encryption. Several activities which involve the domestic dissemination of cryptographic material continue to be prohibited, despite recent amendments.

Courts are now faced with resolution of these issues. Judges have to decide whether the activities involve speech or functional commodities (conduct). The question of whether the controls have a "chilling effect" on speech, and whether the licensing scheme is a prior restraint, must also be answered. If a court decides that the regulations are written overbroadly, it may also have to rule on whether the agency has exceeded its authority. Finally, the question of whether the court has subject matter jurisdiction, given that these are matters of foreign policy and national security, must be resolved. This political question claim, and the fact that the export schemes contain exemptions from judicial review, requires careful consideration of Fifth Amendment due process rights.

\section*{IV. Analysis}

\subsection*{A. Examining the ITAR Provisions}

1. \textit{Key Definitions in ITAR}

The first step is to examine key provisions in ITAR to determine whether they are written so as to include the domestic dissemination of cryptography, or communication about cryptography, which may impinge on the First Amendment.

a. \textit{Export}

Under ITAR, the definition for export includes "s\textsuperscript{ending or taking} a defense article out of the United States in any
manner, except by mere travel outside of the United States by a person whose personal knowledge includes technical data," or "[d]isclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad." 180 The plain meaning of this language indicates that it includes all activity which communicates cryptographic information to a foreign person, even individuals within the United States.

It is this language that the plaintiff in Bernstein finds so objectionable. 181 There, the plaintiff argues that this overly broad language permits the State Department to restrict any and all communications about cryptography, even communication within the United States, and therefore violates the First Amendment. 182

b. Technical Data

The technical data definition may also be too broad to hold any reasonable limitations on the administering agency. "Technical data" is defined as:

(1) Information, other than software as defined in § 120.10(d), which is required for the design development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions and documentation;

(2) Classified information relating to defense articles and defense services;

(3) Information covered by an invention secrecy order;

(4) Software as defined in § 121.8(f) of this subchapter directly related to defense articles;

(5) This definition does not include information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities or information in the public domain as defined in § 120.11. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles. 183

---

180. 22 C.F.R. § 120.17 (1), (4) (1996).
182. Complaint at 11, Bernstein (No. 95-0582).
183. 22 C.F.R. § 120.10 (1996).
In analyzing the ITAR language, one should first consider which activities the regulations prohibit. Does ITAR prohibit (a) an individual printing and distributing an English language analysis of a prohibited source code to friends, (b) source code in print form, (c) source code on a floppy disk, (d) posting source code on the Internet, (e) giving a lecture on cryptographic algorithms at a university, or (f) merely having a conversation at any location about how to write good cryptographic source code, as long as, in (a)-(f) above, the information reaches a foreign national?

The answer is that it is not clear how far the ITAR regulations reach. Scenarios (a), (e), and (f) all appear to be prohibited activities because they involve the items and/or activities of Section (1) for technical data. Indeed, it is difficult to imagine any kind of "information other than software" which would not be included in this first section of the technical data definition.

This ITAR definition of "technical data" was limited by the Ninth Circuit's decision in United States v. Edler, to information "significantly and directly related to specific articles on the Munitions List." The court in Edler sought to narrow the reach of the statute so that it would "avoid serious interference with the interchange of scientific and technological information."

However, the court's attempt to save the regulations from constitutional attack was unsuccessful. Scenario (a), for example, would still likely be prohibited even if the analysis in question did not contain source code, because the analysis is "significantly and directly related to" the source code which is specified on the USML. Additionally, it would not meet the section 5 exclusion clause, if it could not be verified that it was a "general scientific, mathematical or engineering" principle which was "commonly taught." Finally, from the public domain exemption discussed below, it appears that only scenario (e) out of this (a), (e), and (f) grouping, would clearly qualify as information in the public domain, since it is the

---

184. See id. (§ 1 of the technical data definition).
185. 579 F.2d 516 (9th Cir. 1978).
186. Id. at 521.
187. Id.
188. See ¶ (5) of definition supra and text accompanying note 183.
189. See ¶ (5) of definition supra and text accompanying note 183.
only one connected to a university or academic conference setting.

As for scenarios (b) and (c), the distinction between cryptography in print and cryptography in source code form is a problem of interpreting a vague or imprecise regulation. This distinction between information in source code from the same information in print form, is the main issue in Karn.190

For the plaintiff in Karn, the distinction is factually incorrect as well as constitutionally unsound.191 It is also offered as evidence of arbitrary and capricious application of the regulations by the ODTC.192 However, the ODTC has consistently made a distinction between “information” and “technical data” on the one hand and “software” on the other hand.193 “The State Department has construed the regulations in such a way as to effectively eliminate the public domain exemption for software per se.”194 The Karn court did not address this issue directly, dismissing the issue instead on non-justiciability grounds.195

Finally, Scenario (d), posting to the Internet source code which is prohibited for export, would be a violation because, in posting information to the Internet, it clearly would reach not only foreign nationals within the United States, but also foreign persons and countries outside the United States. As such, it would clearly fall within the meaning of several of the sections listed in the “export” definition.196

In sum, the plain meaning of key ITAR definitions indicates that the regulations are capable of restricting the dissemination of ideas on cryptography and communications about cryptography. This can be shown by scenarios (a) and (f), where an individual shares with a friend an analysis of cryptographic source code or has a casual conversation about cryptography. As long as this information is likely to reach a

191. Plaintiff's Opposition at 2-5, Karn (95-01812).
192. Plaintiff's Opposition at 8, Karn (95-01812).
193. Radlo, supra note 175, at 4.
194. Id.
196. One practitioner notes that certain persons have made software available via FTP (file transfer protocol) over the Internet with warnings that foreign persons are prohibited from downloading the software. It is not known yet whether such warnings will have any legal effect because the issue has not been tested in court. Radlo, supra note 175, at 7.
foreign national within the United States or finds its way past United States national borders, ITAR would apply.

2. Incremental Amendments to the ITAR

   a. ITAR Continues to Prohibit Cryptographic Communication

The ITAR have undergone several series of amendments, some of which appear to have been aimed at alleviating constitutional problems associated with these overbroad and imprecise definitions. In 1978, 1981, and 1984, the Department of Justice opined that the ITAR amendments proposed by the State Department would not be sufficient to bring the regulations out of the reach of "speech" under the First Amendment, and might be an infringement.

The most recent revisions to ITAR were focused on the "public domain" exemption. The early "public domain" exemption was limited to unclassified technical data in published form that was available to the public via:

1. Sales at newsstands or bookstores;
2. Unrestricted subscription or purchase;
3. Second class mailing privileges granted by the U.S. Government; or

In 1984, the ODTC expanded this exemption to include "information concerning general scientific, mathematical or engineering principles," and added Section 5 to the "technical data" definition. The revised regulations also exempt technical data approved for release by any United States government agency. In 1993, ODTC further expanded the public domain exception to include unclassified technical data in published form that was available to the public via:

1. Patents available at any patent office;
2. Unlimited distribution at a public conference, meeting, seminar, trade show or exhibition in the US;

---

197. Robinson Memo, supra note 63, at 1 n.1. and 6 n.9.
198. See supra note 63 and accompanying text.
199. See Rubenstein, supra note 20, at 188-89 for a summary of the revisions to the public domain exemption.
200. 22 C.F.R. § 75.48 (1955).
201. 22 C.F.R. § 120.21(c) (1984).
(3) Public release in any form after approval by the cognizant U.S. government agency; and

(4) Fundamental research in science and engineering at US colleges and universities where the resulting information is ordinarily published and shared broadly in the scientific community (this excludes research which is restricted either for proprietary reasons or in connection with funding by the US Government).

The problem with these revised regulations is that it is not clear exactly what is considered to be in the public domain. Critics suggest that the ODTC keeps the public domain exemption vague so that it will have maximum flexibility in turning down commodity jurisdiction applications containing encryption. While the ODTC’s motivations are not entirely clear, what is clear is that, despite the revisions, the ITAR continue to restrict activity that is protected under the First Amendment, and thus can have a chilling effect.

b. Creating Confusion and Failing to Give Adequate Notice

In retaining a vague public domain exemption, the ODTC’s administration of ITAR may have a chilling effect on speech because people do not know what is or is not in the public domain, and hence will refrain from speech that is otherwise protected. Conversely, some persons will assume that software which is in the public domain is freely exportable, and may break the law unintentionally.

A good example of the confusion is provided by ODTC’s position on DES. The DES algorithm plainly meets the public domain exemption. Details of the DES algorithm are freely available from NIST publications and they have been available since 1977. Publication of software programs containing DES are available, and their export in paper form is permitted. Yet, the ODTC does not permit the unlicensed export of products using DES for encryption, other than for two very limited exceptions.

\[204. \text{22 C.F.R. § 120.11 (1994).}\]
\[206. \text{Testimony, supra note 45, at 482.}\]
\[207. \text{Id.}\]
\[208. \text{See supra note 101.}\]
The importance of this example becomes clear if one considers the number of people who may regularly, without any intention, violate the law. If one peruses the Internet "SCI.CRYPT" newsgroup, it appears that many people with an interest in cryptography believe that DES software is in the public domain and thus exportable in any form. At least some of these persons could act upon that belief and post material with a DES algorithm to the Internet, or export it in a product.

In fact, in an often cited instance of illegal export, the government's standards agency, NIST, posted to the Internet an item that contained source code for DES. In paper form, the Automated Password Generation Standard that NIST posted, FIPS 181, is acceptable for worldwide dissemination. The FIPS, available over the Internet without an export restriction notice, was immediately copied by computers in Denmark, the United Kingdom and Taiwan. When this ITAR violation was pointed out, NIST removed it from the directory. The point is that if the government's own agency responsible for standards dissemination can make an error given the ambiguity of the regulations, it is likely that many people can and do make these errors as well.

A second example is provided in Bernstein. In correspondence following his initial CJ application, Bernstein sought clarification as to whether his academic papers were also subject to ODTC jurisdiction. The ODTC responded that all the items submitted were subject to AECA and ITAR licensing. After Bernstein filed his lawsuit, the ODTC sent a letter stating that the academic paper was not subject to the licensing requirement. The court found it "disquieting" that Bernstein's academic paper on the algorithm was apparently subject to licensing for nearly two years and was only reclassified after plaintiff initiated his action.

Although the ODTC has tried to amend the ITAR so that it does not offend the First Amendment, its method of provid-

209. This example is taken from Rubenstein, supra note 20, at 190.
210. Testimony, supra note 45, at 482.
211. Id.
213. Id.
214. Id.
215. Id.
216. Id. at 1434.
ing very narrow exceptions to an overly broad and imprecise regulation has not succeeded in insulating the statute and regulations from constitutional challenges.\textsuperscript{217} ITAR still contains provisions which restrict the dissemination of cryptographic ideas and communications.\textsuperscript{218} It also uses imprecise definitions that are likely to confuse persons engaged in the distribution of cryptography, and thus does not give people adequate notice that their actions are illegal.\textsuperscript{219}

Regardless of whether the government actually applies ITAR to restrict ideas and communications, the language of ITAR permits such restrictions and, thus, the government at some future date may use them for such purposes. Therefore, ITAR leaves the export control regime open to attack on free speech and due process grounds.

B. \textit{Protected Speech and the Appropriate Standard of Review}

Part IV.A established that the AECA and ITAR impose restrictions on an individual’s ability to disseminate cryptography, and on an individual’s ability to communicate about cryptography abroad, and within the United States if that speech can be received by foreign nationals. The next question is, whether these activities are speech which warrants protection under the First Amendment.

1. \textit{Speech or Functional Commodity?}

To be protected under the First Amendment, the prohibited activities must first be determined to be protected speech. In both \textit{Karn} and \textit{Bernstein}, the government argued that its enforcement of the AECA under ITAR does not regulate speech at all, but only conduct.\textsuperscript{220} It characterized the conduct as an application for an export license, and proposed that the material submitted is software, which has a functional rather than a communicative purpose.\textsuperscript{221}

\begin{itemize}
\item \textsuperscript{217} See supra part IV.A.2.
\item \textsuperscript{218} See discussion supra part IV.A.1.
\item \textsuperscript{219} See discussion supra part IV.A.2.b.
\item \textsuperscript{220} See, e.g., Memorandum of Points and Authorities in Support of Defendants’ Motion to Dismiss at 2, Bernstein v. United States, 922 F. Supp. 1426, 1430 (N.D. Cal. 1996) (No. 95-0582).
\item \textsuperscript{221} See discussion supra part IV.A.1.
\end{itemize}
Relying on its characterization that the regulated activity in *Karn* and *Bernstein* was conduct not speech, the government proposed the *United States v. O'Brien* standard to determine the constitutionality of the AECA and ITAR. The *O'Brien* standard is that an incidental restriction on speech will be permitted if (1) it is within the constitutional power of the government, (2) it furthers an important or substantial government interest, (3) the governmental interest is unrelated to the suppression of free expression, and (4) the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.\(^223\)

The *Bernstein* court rejected the government’s argument, finding that the source code was speech for purposes of the First Amendment.\(^224\) In addition, the court did not accept the *O'Brien* test as the appropriate standard.\(^225\) The court noted that the test was probably inapplicable to situations where the activity at issue was determined to be speech not conduct.\(^226\) The *Bernstein* court also found that the government was unconvincing on the third and fourth prongs of *O'Brien* because “regulating cryptographic software appeared to relate to ‘the suppression of free expression’ and may reach farther than is justifiable”.\(^227\)

In contrast, the *Karn* court “made no ruling as to whether source codes ... fall within the protection of the First Amendment”\(^228\) and stated that it would “assume that the protection of the First Amendment extends to the source code”\(^229\) for the purposes of deciding whether the regulation was justified.

However, the *Karn* court’s reasoning contradicts its assumption that the source code is protected speech. The fundamental problem with the court’s analysis in *Karn* is that its acceptance and use of the *O'Brien* test undermines its stated assumption. On the one hand, the court states that it as-

\(^222\) 391 U.S. 367 (1968).
\(^223\) Id. at 377.
\(^224\) *Bernstein*, 922 F. Supp. at 1436.
\(^225\) Id. at 1437.
\(^226\) Id.
\(^227\) Id.
\(^229\) Id. at 9.
sumes cryptographic source code is speech for its First Amendment analysis. At the same time, however, it selects the O'Brien standard, a First Amendment test which is applicable to conduct, not speech cases.\textsuperscript{230}

By utilizing this standard, the Karn court has in effect assumed that the government is regulating conduct, which incidentally impacts speech. The court's selection of the differential O'Brien standard is consistent with other sections of the opinion that treat the source code not as speech, but as a functional commodity, which the court assumes Karn was attempting "to export" for profit.\textsuperscript{231}

2. The Appropriate Standard of Review

Establishing that the dissemination of one's cryptographic source code is protected speech, however, is not the end of the inquiry. Restrictions on speech, even prior restrictions, are not per se unconstitutional.\textsuperscript{232} The court must look carefully at the government's rationale for the restraint to decide if the licensing scheme is justified under the circumstances.\textsuperscript{233}

Two inquiries are relevant to deciding whether the AECA and ITAR scheme violate the First and Fifth Amendments: (1) the distinction between content-based v. content-neutral regulations, and (2) prior restraint analysis. Examining the AECA and ITAR under Supreme Court doctrine developed in these First Amendment areas will determine the level of scrutiny the court should apply.

a. The Content-Based v. Content-Neutral Distinction

Whether a regulation of speech is permitted depends in part upon whether the restriction is content-based or content-neutral.\textsuperscript{234} Content-based restrictions regulate speech on the basis of its general subject matter or on the basis of its partic-

\textsuperscript{230} See Harmon Memo, supra note 58, at 543 n.16; cf. Clark v. Community for Creative Non-Violence, 468 U.S. 288, 298 (1984) (equating the lesser scrutiny standard for expressive conduct cases such as O'Brien with time, place and manner restriction cases).

\textsuperscript{231} Karn v. United States, 925 F. Supp. at 2.

\textsuperscript{232} See Near v. Minnesota ex rel. Olson, 283 U.S. 697, 716 (1931).


\textsuperscript{234} See generally Laurence H. Tribe, American Constitutional Law 802 (2nd ed. 1988).
ular viewpoint. "Content-neutral restrictions limit expression without regard to the content or communicative impact of the message conveyed." Except for speech that the Supreme Court has determined is of low First Amendment value, content-based regulations warrant strict scrutiny and are generally held unconstitutional.

In contrast, the Supreme Court has applied a host of different standards to content-neutral regulations, which correspond roughly to deferential, intermediate and strict scrutiny review. The difficulty in sorting through the case law on content-neutral regulations is that the Supreme Court does not speak overtly of these three standards of review and it has not precisely defined them. However, it would be incorrect to conclude that all content-neutral regulations warrant deferential scrutiny. The Supreme Court has frequently used the intermediate and strict standards for content-neutral regulations.

The Karn court decided that the AECA and ITAR scheme is content-neutral and accepted the government's deferential O'Brien standard. Unfortunately, the Karn opinion arrived at this standard of review without any analysis of whether the regulation is content-based and without any consideration of whether a different scrutiny standard other than the deferential O'Brien test applied to content-neutral regulations.

235. See id at 803.
237. Certain categories of speech, such as obscenity, have been determined to be of low First Amendment value. Jill M. Ryan, Note, Freedom to Speak Unintelligibly: The First Amendment Implications of Government-Controlled Encryption, 4 WM. & MARY BILL RTS. J. 1165, 1189-99 (1996).
238. Id. at 1200.
239. Stone, supra note 236, at 48-54. Stone has found the Supreme Court to articulate at least seven seemingly different standards for content-neutral review. However, his analysis shows that they collapse into these three. Id. The O'Brien test is considered a highly deferential review standard. Id. at 51.
240. Id. at 53-54.
241. See id. at 48-54
242. Stone, supra note 236, at 54.
244. Id. at 9-12.
245. Id.
The *Karn* opinion merely presents arguments as to why the regulation is content neutral and then proceeds to apply the *O'Brien* test. In so doing, the decision leaves the content-based v. content-neutral analysis incomplete. In contrast, the *Bernstein* court, recognizing that the parties had not had the opportunity to brief the court on the applicable First Amendment standard, specifically noted that it would make no decision on the appropriate standard. Instead, it made the limited ruling that source code was protected speech and that the plaintiffs' claims were colorable even under the *O'Brien* test put forth by the government.

There is, however, a strong argument that the AECA and ITAR scheme is a content-based regulation. Content-based regulations extend to restrictions on public discussion of an entire subject or topic. The technical data and export definitions of the ITAR are so broad as to include the entire subject of cryptography. If the information could potentially reach a foreign national, or if it could find its way to the Internet, it requires a license. And, although the scheme allows some communication of cryptographic information, namely that which is in the public domain, it is not clear, even to government officials at the ODTC and NIST, what is in the public domain. Thus, the ITAR scheme requires one to submit a CJ application and obtain a license prior to disseminating any cryptography, unless the speaker can carefully control where the cryptography ends up.

247. Id.
248. Id. at 1437.
249. See Consolidated Edison v. Public Serv. Comm'n, 447 U.S. 530 (1980) (where the Court prevented a public service commission from ordering utilities not to discuss in their monthly billing materials the desirability of nuclear power).
250. See supra part IV.A.1 and accompanying notes. Cryptography is generally defined as the art and science of keeping messages secure.
251. For almost three years, the Department of Justice was prosecuting Phil Zimmerman for precisely this offense. Zimmerman shared with others interested in cryptography his PGP (Pretty Good Privacy) software for encryption. Some of these persons posted PGP to the Internet. In January of 1996, the Department of Justice decided to drop the investigation of Phil Zimmerman. See Radlo, supra note 175, at 7.
252. See part IV.A.2.b.
253. While it is true that persons can freely discuss, for example, their social or political opinions on cryptography, this does not detract from the argument
This distorts the public debate on cryptography in a content differential manner in at least two ways. First, it removes a certain amount of public debate from the “marketplace of ideas.” It will chill some cryptographic speech because some people will not want to take the chance of sharing their cryptography with friends or with other cryptographers on the Internet for fear that it will bring prosecution. Second, the regulation requires the speaker to carefully examine their cryptographic communications to decide what is and is not subject to the regulation based on its content.254

Even if the AECA and ITAR are categorized as content-neutral, the Court may select a higher scrutiny standard than the deferential O'Brien standard if it feels that the regulations reduce opportunities for free expression.255 The Supreme Court has long recognized that by limiting the availability of a particular means or mode of communication, content-neutral restrictions can significantly impair the ability of individuals to communicate their views to one another.256 In fact, the Court’s pattern has been to use a strict scrutiny standard where a restriction has a relatively severe impact on opportunities for free expression and lesser standards where the impact is significant or modest.257

"The pivotal inquiry in content-neutral analysis is the extent to which particular restrictions actually diminish the opportunities for free expression."258 The court will have to engage in some analysis of how much speech is being curtailed and will likely engage in a balancing between the government and speaker’s interests.259

---

254. One must evaluate whether the cryptography contains the DES or RSA algorithm of sufficient key length or some other restricted algorithm to determine whether one's communication is subject to the regulation. See supra part II.B. This situation is similar to that in City of Cincinnati v. Discovery Network, Inc. 507 U.S. 410, 429 (1993), where an ordinance banning newsracks distributing commercial publications from public sidewalks while allowing newsracks distributing newspapers was determined to be content-based.

255. See Stone, supra note 236, at 57-58.

256. Stone, supra note 236, at 57. The particular mode of communication that the restrictions are impacting in this case is private speech in electronic communications.

257. Id. at 57-58.

258. Id. at 77.

259. Id. at 77-78.
The essential question for a balancing analysis is who should bear the burden of the conflict between the speaker and the regulation. "Should the speaker have to shift to alternative means of communication or should the government have to shift to alternative means of achieving its objectives?" To the extent it can be shown that speakers cannot shift because any mode of cryptographic communication that reaches a foreign national is potentially violative, the government regulation should be struck.

The ITAR restrictions could also be seen to pose an undue burden on the speaker to shift to another mode of communication, thus limiting the opportunities for free expression. For example, many people interested in cryptography use the "SCI.CRYPT" newsgroup on the Internet to communicate their ideas to one another. This means of communication is very efficient and inexpensive, allowing anyone with Internet access to participate in technical discussions on cryptography. It is in this forum, however, that sharing one's cryptography is violative of ITAR regulations because posting to the Internet "exports" the cryptography. If the ODTC stringently enforced the ITAR provisions, the opportunities for free expression for many amateur cryptographers would be significantly curtailed.

b. Prior Restraint Analysis and Due Process

 Bernstein argues that requiring a license before one can publish ideas in a way which reaches a foreign national is a prior restraint on speech, and therefore the government, in order to prevent speech, must bear the heavy burden placed on it in recent First Amendment prior restraint cases. Prior restraints on publication are permissible only in extreme circumstances. The Supreme Court, in New York Times, decided that the test is that there must be a showing that disclosure "will surely result in direct, immediate and irreparable damage to our Nation or its people." In applying this test, the court will have to decide whether allowing

260. Id.
261. See note 196 and accompanying text.
262. New York Times Co. v. United States, 403 U.S. 713 (1971). This case is also referred to as The Pentagon Papers.
cryptographic communication will result in "direct, immediate and irreparable damage." 265

If the court decides that the AECA and ITAR are a prior restraint, it is unlikely that the restrictions would meet the strict *New York Times* standard, or even an intermediate scrutiny standard. The harm which can be directly attributed to the release of cryptographic information is almost negligible. While one can postulate a very indirect connection between the ability of the NSA to carry out its signals intelligence tasks and the release of strong cryptography into the public domain, this indirect connection does not rise to a heightened scrutiny standard.

c. The Effectiveness of ITAR

The effectiveness of the government's restrictions are also a problem under a higher scrutiny standard. Many people have pointed out that export controls cannot limit the spread of strong cryptography to any reasonable degree, because so many persons outside the United States already have strong cryptography. 266 Since cryptography is so readily available overseas, the government's interest could only be in slowing its dissemination. All the government accomplishes by preventing the spread of better cryptographic techniques is a small increase in the cost to other nations of using encryption which is good enough to keep the NSA from accessing their communications. Since strong cryptography is generally available abroad and relatively inexpensive, 267 it is very hard to conceive of a situation where such an effect would rise to the standard of harm outlined in *New York Times*.

d. Freedman v. Maryland: The Free Speech and Due Process Standard

The *New York Times* standard of harm is not the only hurdle under a prior restraint analysis, because of the due process implications. "Even in those limited circumstances in which prior restraints have been deemed constitutionally permissible, they have been circumscribed by specific, nar-

265. *Id.*

266. See supra note 48 and accompanying text for how widespread strong cryptography is worldwide.

267. See Evans, supra note 35 at 469.
narrowly drawn standards for deciding whether to prohibit disclosure and by substantial procedural protections. "268 The government can require a license for speech only if there is an important reason for licensing, and clear criteria leaving almost no discretion to the licensing authority. 269 Licensing must contain procedural safeguards, such as prompt determination of requests for licenses and judicial review of license denials. 270

In Freedman, the Supreme Court set out the procedural protections required to uphold a system of prior review:

1. A valid final restraint may be imposed only upon a judicial determination;
2. The administrator of a licensing scheme must act with a specified brief period of time;
3. The administrator must be required either to issue a license or go to court to seek a restraint;
4. Any restraint imposed in advance of a final judicial determination on the merits must be limited to preservation of the status quo for the shortest period compatible with sound judicial resolution; and,
5. The licensing scheme must assure a prompt final judicial decision reviewing any interim and possibly erroneous denial of a license. 271

Freedman essentially dictates that the measure of due process required for the First Amendment is a full hearing by a court before any prior restraint can be imposed. 272 The licensing decision must be subjected to a prompt judicial review in a proceeding in which the government will bear the burden of justifying its decision. 273 Thus, the burden of bringing a judicial proceeding cannot be imposed upon those desiring export licenses to communicate cryptographic speech, as is currently the case under the AECA and ITAR.

The AECA export scheme fails to provide the procedural protections given in Freedman. 274 The AECA and ITAR, as interpreted by the ODTC, do not provide this level of due pro-

268. Harmon Memo, supra note 58, at 542.
270. See Freedman, 380 U.S. at 59-61.
271. Id. at 58-59.
272. See supra note 155 and accompanying text.
273. See supra note 155 and accompanying text.
cess because there is no opportunity for appeal outside of the administering agency. Instead, the government may deny permission as it sees fit, without any administrative or judicial hearing, and without a time limit for a final decision.

The court should review the claims applying the Freedman and New York Times standards. The level of judicial scrutiny given by this First and Fifth Amendment jurisprudence conflicts with both the AECA's statutory preclusion of judicial review and non-justiciability on political question grounds.

C. Judicial Review

The cryptography First Amendment cases differ from the more mainstream First Amendment line of cases in a very important way. The courts must contend with arguments that the claims are not reviewable because of statutory preclusions in the export laws and because the claims concern a political question, and are thus not within the federal courts' subject matter jurisdiction.

1. The Statutory Exemption

The AECA contains a specific provision for a limited exemption from judicial review, which reads as follows:

Judicial review of designation of items as defense articles or services.

The designation by the President (or by an official to whom the President's functions under subsection (a) of this section have been duly delegated), in regulations issued under this section, of items as defense articles or defense services for purposes of this section shall not be subject to judicial review.

275. See discussion supra part II.B.3.c.
276. See notes 140-42 and accompanying text.
277. On the government's motion to dismiss under Federal Rule of Civil Procedure 12(b)(6), a court will usually hear the political question issue prior to addressing the case on the merits. A claim may "arise under the Constitution" by presenting constitutional questions yet still be non-justiciable. In this case, the court would invoke Federal Rule of Civil Procedure 12(b)(1), lack of jurisdiction over subject matter. See Paul Brest and Sanford Levinson, Processes of Constitutional Decisionmaking: Cases and Materials 1466 (1992).
Thus, any court hearing First and Fifth Amendment challenges to the AECA must consider to what extent this statutory language precludes consideration of the claims.

a. Constitutional Claims

There is a strong presumption under administrative law that Congress intends judicial review of administrative action. Subject to constitutional constraints, Congress can make exceptions to the historic practice whereby courts review agency action. The presumption of judicial review is, after all, a presumption, and "like all presumptions used in interpreting statutes, may be overcome by," inter alia, "specific language or specific legislative history that is a reliable indicator of congressional intent to preclude judicial review that is fairly discernible" in the detail of the legislative scheme. Where substantial doubt about the congressional intent exists, the general presumption favoring judicial review of administrative action is controlling.

Unfortunately, almost no legislative history is available for the §2778(h) exemption that was passed as an amendment to the AECA in 1989. The Congressional intent underlying the passage of this amendment is vague, at best. Furthermore, the legislative history and case law on the reach of the §2778(h) exemption provides even less clarity. Both Karn and Bernstein ruled that the AECA statutory exemption does not preclude constitutional claims.

Where Congress intends to preclude judicial review of constitutional claims its intent to do so must be clear... [This] heightened showing [is required] in part to avoid the "serious constitutional question" that would arise if a federal statute were construed to deny any judicial forum for a colorable constitutional claim.

281. Id.
b. Administrative Claims

However, the Karn and Bernstein courts took very different approaches on the justiciability of administrative or "abuse" claims. The Karn court viewed the plaintiff's APA and ultra vires claims as a challenge to the ODTC's CJ decision that the material on the disk was not in the public domain.\textsuperscript{286} As such, the court held the §2778(h) exemption barred the claim because this statutory exemption extends to all decisions regarding the CJ procedure.\textsuperscript{287} The court distinguished Karn's challenge of the CJ decision from a "facial challenge" to the statute, which raises "a discrete issue, unrelated to the facts of the case, that only needs to be resolved once."\textsuperscript{288}

In contrast, the Bernstein court argued that in addition to constitutional claims, ultra vires or "abuse" claims were also outside the statutory preclusion.\textsuperscript{289} Unlike the Karn court, Bernstein did not dismiss plaintiff's APA or administrative claims.\textsuperscript{290}

In finding all challenges to the CJ procedures subject to the judicial review preclusion, the Karn court has construed the §2778(h) preclusion broadly to restrict all types of claims which can be brought under §2778(h), except those based upon strictly facial constitutional challenges. Yet, there is no case law supporting this narrow reading of the effect of the 2778(h) statutory preclusion or any of the statutory preclusions under the export control laws. Moreover, the Bernstein court demonstrated that case law exists to establish that such claims are not subject to the statutory preclusions in the export control laws.\textsuperscript{291}

2. The Political Question Doctrine

The courts have been reluctant to hear the First and Fifth Amendment challenges against AECA and ITAR because of the political question doctrine. However, there are

\textsuperscript{286} Karn, 925 F. Supp. at 5-8.
\textsuperscript{287} Id. at 6.
\textsuperscript{288} Id. at 8.
\textsuperscript{290} Id. at 1437.
\textsuperscript{291} See supra note 289.
several arguments in support of judicial review, even though the claims relate to national security concerns.

It is well established under the political question doctrine that courts do not possess the expertise to examine sensitive political questions reserved for the elected branches of government.\textsuperscript{292} The government argued in \textit{Karn} and \textit{Bernstein} that the determination of whether an item should be on the USML "possesses nearly every trait that the Supreme Court has enumerated traditionally renders a question 'political'."\textsuperscript{293} The \textit{Bernstein} court, however, argued that a review of a CJ determination was "distinctly different" from a constitutional challenge and "the judicial branch not only possesses the requisite expertise to adjudicate these issues, it is also the best and final interpreter of them."\textsuperscript{294}

"The doctrine is one of 'political questions' not one of 'political cases'."\textsuperscript{295} The court should not reject a bona fide controversy as to whether some action denominated 'political' exceeds constitutional authority.\textsuperscript{296} Federal courts have consistently addressed constitutional issues in the context of national security concerns.\textsuperscript{297}

The limited statutory exemption from judicial review provided by AECA 2778(h) and the political question doctrine must be considered against the plaintiffs' right to free speech and due process prior to being denied life, liberty, or property. Even if the government interest in regulating the flow of cryptographic information is significant enough to warrant some form of prior restraint, the government should provide prompt, expedited judicial review before imposing the restraint, as established in \textit{Freedman}. The rulings of courts that have shown judicial restraint in deciding First and Fifth Amendment cases against the AECA have not adequately settled the issue. The \textit{Edler} court, for example, attempted to resolve the constitutional difficulties in the ITAR regulations by narrowing the scope of

\begin{small}
\begin{itemize}
\item \textsuperscript{292} \textit{See} Baker v. Carr, 369 U.S. 186 (1962).
\item \textsuperscript{293} \textit{Bernstein}, 922 F. Supp. at 1431 (quoting United States v. Martinez, 904 F.2d 601, 602 (11th Cir. 1990)).
\item \textsuperscript{294} \textit{Bernstein}, 922 F. Supp. at 1431.
\item \textsuperscript{295} Nuclear Pacific, Inc. v. United States, No. 84-49R, slip op. at 7 (W.D. Wash. June 8, 1984) (citing \textit{Baker}, 369 U.S. at 217).
\item \textsuperscript{296} \textit{See id}.
\item \textsuperscript{297} \textit{Bernstein}, 922 F. Supp. at 1431 (citing New York Times Co. v. United States, 403 U.S. 713 (1971) and Haig v. Agee, 453 U.S. 280 (1981)).
\end{itemize}
\end{small}
the technical data provisions. It made this attempt by restricting the regulations to information "that relate[s] in a significant fashion to some item on the Munitions List." However, as discussed, this attempt did not put any meaningful limits on the definitions.

V. RECENT DEVELOPMENTS

Two events occurring in December of 1996 altered the landscape of encryption export controls and require additional analysis. The first is that the Bernstein court declared Category XIII(b) of the ITAR unconstitutional as a prior restraint on speech. The second is that on December 30, 1996, the Clinton Administration transferred export jurisdiction over non-military encryption from the USML to the CCL, amending the EAR. Although these two recent developments are only the latest in the continuing political struggle over encryption, they will substantially impact lawmakers and administrators charged with the task of resolving these issues.

A. Bernstein Declares the AECA/ITAR Scheme as Applied to Cryptography Unconstitutional

Although not a surprising result under the analysis in Part IV, the Bernstein court's decision, released December 18, 1996, was headline news. In sharp distinction to the Karn decision, the Bernstein court ruled that Category XIII(b) was "directed very specifically at applied scientific research and speech on the topic of encryption," and thus could be considered a content-based regulation. The fact that the
scheme regulates encryption in the interest of national security did not alone justify a prior restraint for the court, which relied heavily on New York Times.\(^{306}\)

More importantly, however, the court found that the AECA and ITAR licensing scheme was an unconstitutional prior restraint because it did not meet the Freedman procedural standards in failing to provide: (1) a time limit on the licensing decision, (2) prompt judicial review, and (3) a duty on the part of the ODTC to go to court and defend a denial of a license.\(^{307}\)

Although the Bernstein court voided sections of the public domain exemption as applied to technical data,\(^{308}\) it took a rather conservative approach in striking the other ITAR definitions. The court declared Category XIII(b) unconstitutional and the technical data definition unenforceable, but only as it relates to items in Category XIII(b), in order to extend its invalidation of the statute no “further than is necessary to dispose of the case before it.”\(^{309}\) While the court found certain ITAR provisions failed to give people “a reasonable opportunity to know what was prohibited,”\(^{310}\) and uncertainty in what acts can actually be prosecuted under the ITAR, it did not find the “export” definition “impermissibly vague.”\(^{311}\)

B. Jurisdictional Shift from the USML to the CCL

Responding to software industry pressure for encryption export control reform, and possibly in anticipation of an unfavorable Bernstein decision, the government put into effect regulations shifting export control from the State Department’s ODTC to the Commerce Department’s BXA.\(^{312}\) Executive Order 13026 “amends the EAR by imposing national security and foreign policy controls (“EI” for Encryption Items) on certain information security systems and equipment, cryptographic devices, software and components specifically

\(\text{306. Id. at 8.} \)
\(\text{307. Id. at 10.} \)
\(\text{308. Id. at 14.} \)
\(\text{309. Bernstein, 1996 WL 730283, at *10-15.} \)
\(\text{310. Id. at 14.} \)
\(\text{311. Id.} \)
\(\text{312. See supra note 302 and accompanying text.} \)
designed or modified therefor, including recoverable encryption software, and related technology ("encryption items").

Essentially, the amendments add new EI controls under Export Commodity Control Numbers (ECCN) 5A002, 5D002 and 5E002 for "commodities, software and technology". While the most recent changes to the ITAR required licensing of 40 bit or greater encryption, the new amendments to the EAR subject encryption to five different categories of licensing:

1. Certain mass market encryption software after a one time BXA review may be released from controls;
2. Recovery encryption software and commodities may be eligible for a license exception after a one time BXA review;
3. Non-recovery EI's up to 56 bits DES or the equivalent requires a general licenses after a one time BXA review if the exporter agrees to build and market a "key-recovery escrow" system that would allow the government access to encrypted data;
4. All other encryption will be subjected to an "encryption licensing arrangement" which is intended to continue without change the regulatory treatment of the ITAR; and
5. Encryption technology exports which will be considered on a case-by-case basis.

These amendments, particularly the new provisions for 56 bit encryption for a period of two years, were an implementation of a compromise between the software industry and the Clinton Administration. In exchange for a commitment by the industry to develop key escrow—which places the key in escrow with a trusted, government approved third
party, who could provide access to government law enforcement agencies—the government agreed to ease export controls. Instead, the new regulations have been viewed by software industry representatives and civil libertarian groups as “a government shell game”. They insist that the new export rules are virtually identical to the AECA/ITAR scheme.

C. The Jurisdictional Shift Does Not Resolve the Constitutional Issues

The regulatory shift by the Clinton Administration fails to resolve the constitutional issues posed by Bernstein and Karn. The new regulations continue to violate the First Amendment because they are content-based and fail to provide the procedural safeguards required by Freedman.

The Bernstein court considered Category XIII(b) of ITAR a content-based restriction because it was specifically directed at speech on a particular subject matter—cryptography. The court also relied on Supreme Court doctrine that First Amendment protection extends not only to viewpoint prohibitions but also to prohibitions on public discussion of an entire topic. Like Category XIII(b), the Clinton Administration's amendments to the EAR specifically target cryptography and also sweep into EAR control cryptographic speech on this entire topic. As a result, the new regulatory regime violates the First Amendment, just as Category XIII(b) of the ITAR does.

The Bernstein court found the AECA and ITAR licensing scheme to be unconstitutional as a “paradigm of standardless discretion” because it failed three important criteria set out in Freedman: provisions for time limits, prompt judicial re-

321. Id.
322. In addition, the new policy introduces a number of new statutory issues in its attempt to dictate industrial policy, which are beyond the scope of this comment. See Froomkin, supra note 316 (showing that this industrial policy is beyond the statutory authority granted under the IEEPA).
324. Id. at 8.
325. See supra notes 313-21 and accompanying text.
view, and a duty on the part of the agency to go to court to defend its licensing decision.\textsuperscript{326} Similarly, the new regulations under the EAA/EAR fail to comply with \textit{Freedman}. Although the EAR does provide time periods for a licensing decision, it contains no time limit for an appeal.\textsuperscript{327} There is no provision for prompt judicial review of decisions because the EAA contains an explicit exemption from judicial review of agency decisions as does the EAR.\textsuperscript{328} And, of course, with this explicit preclusion of judicial review, the EAA/EAR does not specify a duty on the part of the agency to go to court to defend license denials.

The EAA/EAR licensing scheme \textit{prior to} the Administration's December 1996 amendments did provide certain foreign availability review procedures, which may have been sufficient to keep that regulatory regime in constitutional conformance.\textsuperscript{329} However, the Administration included specific language in its Executive Order 13026 amendments to ensure that the amended EAR would not provide these procedural opportunities.\textsuperscript{330} In its Executive Order 13026 amendments, which pertain only to encryption items, the Administration has effectively continued the licensing regime under the AECA and ITAR, extending unconstitutional provisions on judicial review to the EAA and EAR scheme.

D. \textbf{Statutory Authority Under the IEEPA's Extention of the EAA}

Further complicating the current regulatory status of encryption is the status of the EAA itself. Statutory authority for the EAA, which is essentially a temporary statute, expired in August 1994.\textsuperscript{331} As presidents before him have done

\begin{itemize}
\item \textsuperscript{326} See supra note 307 and accompanying text.
\item \textsuperscript{327} 15 C.F.R. § 756.2(c)(1) provides only that the appeal decision be made within a "reasonable time".
\item \textsuperscript{328} 50 U.S.C. app. § 2412(a); 15 C.F.R. 756.2(c)(2).
\item \textsuperscript{329} Although no cases prior to Bernstein and Karn specifically addressed cryptography and the First Amendment under the EAA and EAR, there are cases which have upheld the EAA/EAR's exemption from judicial review. United States v. Mandel, 914 F.2d 1215, 1220 (9th Cir. 1990); United States v. Helmy, 712 F. Supp. 1423, 1428-29 (E.D.Cal. 1989). While the reasoning in these cases relied primarily on political question grounds, the EAA's review procedures for foreign availability weighed heavily in the analysis. See, e.g. Helmy, 12 F. Supp. at 1433.
\item \textsuperscript{330} 50 Fed. Reg. 68,572,68,575.
\item \textsuperscript{331} Exec. Order No. 12,924, 59 Fed. Reg. 43,437(1994).
\end{itemize}
upon the lapse of statutory authority for the EAA, President Clinton declared a national emergency and issued Executive Order 12924 "in light of the expiration of the Export Administration Act of 1979" and in view of the "unusual and extraordinary threat to national security, foreign policy, and economy of the United States."\(^{332}\)

Executive Order 12924 rests on the authority vested in the President by "the Constitution and laws of the United States of America, including but not limited to section 203 of the International Emergency Economic Powers Act (50 U.S.C. 1702)" (IEEPA).\(^{333}\) The problem with this temporary extension of the EAA is that it is not clear what substantive authority the IEEPA gives to the President to control encryption.

Although Section 1702, defining Presidential authority under the IEEPA, gives sweeping powers to the President over financial transactions and property, the statutory construction of this section and specific language limiting presidential authority over the flow of information indicates that the IEEPA was not intended to allow the regulation of encryption.\(^{334}\)

Throughout the section granting authority, the statute refers to "transactions"\(^{335}\) and "transfers or payments"\(^{336}\) or "property"\(^{337}\) as the objects of regulation. More specifically, Section 1702(b) states that:

\[
\text{[t]he authority granted to the President by this section does not include the authority to regulate or prohibit, directly or indirectly (1) any postal, telegraphic, telephonic, or other personal communication, which does not involve a transfer of anything of value; . . . (3) the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informa-}
\]

---

332. Id. At least one commentator has suggested that the "unusual and extraordinary threat" seems to be Congress's failure to renew the EAA. Froomkin, supra note 316 (showing that this industrial policy is beyond the statutory authority granted under the IEEPA).


The section prohibiting control over the free flow of information goes on to provide an exception for exports “otherwise controlled” by the EAA and national security controls.\textsuperscript{339}

In sum, the IEEPA does not give the President any new statutory authority to control encryption exports. In addition, the structure and language of the IEEPA indicates that the IEEPA does not authorize the President to prohibit the exportation of publications. This is precisely the administrative activity challenged in the \textit{Bernstein} litigation which the federal court ruled unconstitutional. The President should not be allowed to grant himself, by executive order under the IEEPA, emergency statutory authority for administrative action which a federal court has already determined to be an unconstitutional prior restraint on speech. If an administrative action is unconstitutional under a statute, it is also unconstitutional under a Presidential executive order.

The Administration’s uncertain statutory authority under the IEEPA will likely spawn even more litigation by plaintiffs such as Karn and Bernstein, challenging the statutory authority of the Commerce Department to administer export controls on encryption under the EAA/IEEPA and EAR regulatory scheme. Unlike the AECA/ITAR, the EAA/IEEPA scheme is clearly subject to judicial review.\textsuperscript{340} The IEEPA may even allow challenges to the EAA/EAR scheme that would not be judicially reviewable if statutory authority currently existed for the EAA.\textsuperscript{341}

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{338} 50 U.S.C. §1702(b)(1) and (3).
\item \textsuperscript{339} The section reads “otherwise controlled for export under section 2404 of the Appendix to this title, or under section 2405 of the Appendix to this title to the extent that such controls promote the nonproliferation or antiterrorism policies of the United States, or with respect to which acts are prohibited by chapter 37 of Title 18”. \textit{Id.}
\item \textsuperscript{340} Nuclear Pac., Inc. v. Department of Commerce, No. C84-49R slip op. (W.D. Wash. June 8, 1984) (holding that the IEEPA extension of the EAA permits judicial review).
\item \textsuperscript{341} \textit{Id.} at 5. The court held that the IEEPA did not grant the President the power to limit the jurisdiction of the courts. \textit{Id.} Thus, President Clinton’s Executive Order 13026 EAR amendment denying judicial review exceeds the authority granted by Congress under the IEEPA. Because there is no statutory authority to deny judicial review under the IEEPA and no statutory authority to deny judicial review under the EAA because it is a lapsed statute, then there are currently no statutory limitations on the judicial reviewability of claims brought against the EAA/IEEPA and EAR scheme.
\end{itemize}
\end{footnotesize}
Unless Congress acts, further litigation can be expected, with courts potentially striking offending language in the AECA/ITAR or EAA/EAR schemes in order to bring them into constitutional conformance. The result will likely be a regulatory nightmare for both exporters and regulators alike.

VI. PROPOSAL

A. Legislative Reform of Export Control

The Administration has preempted, for the moment at any rate, the Bernstein and Karn litigation currently before the federal courts by removing encryption from AECA and ITAR jurisdiction. The shift in jurisdiction, however, has failed to provide a workable solution for the software industry and to solve the constitutional problems raised by recent litigation because most of the licensing features of the AECA and ITAR have been continued in the EAA/IEEPA and EAR scheme.

Some observers feel that it is up to Congress to make the next move in this political struggle. Software industry representatives have stated publicly that "[their] members agree that [they] should go back to Capitol Hill" for a resolution.

Congress can respond in at least two ways: (1) by passing legislation to renew the EAA and giving the Administration new statutory authority for its EAR amendments; or (2) by enacting entirely new legislation specifically written to effect encryption export control reform. This author recommends that Congress take the latter course and pass legislation specifically providing for export control over encryption which meets the First Amendment strict scrutiny standard of New York Times and the procedural requirements of Freedman.

343. See supra part V.B.
344. See supra part V.C.
347. See discussion supra part IV.B.
Legislation for encryption control reform was submitted in Congress's last session, and is likely to be submitted again in the 105th Congress. If Congress fails to enact reform, the existing ITAR or EAR schemes will continue to operate as a prior restraint on cryptographic speech, and the constitutional problems will remain. In such a case, the courts will be forced to re-examine the constitutional issues in light of the recent developments.

B. Further Judicial Action to Bring Export Controls Into Constitutional Conformance

If Congress fails to enact encryption export control reform legislation, then the court's will be faced with more litigation on these constitutional issues. As of this writing, such challenges will be directed at the EAA/IEEPA and EAR scheme. Claims will be directed at the AECA and ITAR scheme if export controls on encryption are returned to the USML, as President Clinton has threatened to do if Congress enacts export legislation which the Administration deems inadequate.

In either case, further judicial action may be necessary to ensure that export controls on encryption are held to the First Amendment strict scrutiny standards. Two federal district courts have come to opposite conclusions on the constitutionality of export controls, based on AECA and ITAR jurisdiction, leaving the status of the scheme in question.

In the future, courts hearing these cases should continue to strike offending sections of the export controls to bring the regulations in line with constitutional protections on free speech and due process. As the Bernstein decision has demonstrated, it is not necessary for the courts to strike either the statute or the regulations in their entirety. Courts hearing ITAR challenges should, however, go one step farther than the Bernstein court. In addition to striking Category XIII(b), they should strike the three definitions in the ITAR that are unconstitutional on their face: The export, technical

348. See supra note 7.
349. See supra parts IV.B, V.C.
351. See discussion supra part IV.B.
352. See discussion supra part V.A.
data, and public domain exemption sections.\textsuperscript{353} The ODTC should be required to narrow the scope of these three definitions so that they do not apply to the types of situations analyzed in scenarios (a) through (f).\textsuperscript{354}

By far the most important element missing in both the AECA/ITAR and EAA/IEEPA and EAR schemes from both a prior restraint and a due process analysis, is a clear provision for a judicial determination before a final restraint is imposed.\textsuperscript{355} The judicial exemptions should be interpreted narrowly so that constitutional and administrative "abuse" claims can be heard.\textsuperscript{356} The court should also interpret the statute to provide for full, expedited judicial review which meets the \textit{Freedman} standard.\textsuperscript{357}

\section*{VII. Conclusion}

The legislative and regulatory stalemate over government encryption policy has essentially left to the federal courts the task of resolving First and Fifth Amendment claims against export controls on encryption. Although the judiciary is not the best forum for legislative and regulatory reform, courts are uniquely equipped to decide constitutional questions.

Because source code is speech and because the export controls are both content-based regulations and prior restraints on speech, federal courts hearing the First and Fifth Amendment claims should use a strict scrutiny standard and review cases under the more stringent \textit{Freedman} and \textit{New York Times} tests. Substantial revisions to the export control laws are required. Thus, Congress should pass comprehensive reform legislation, rather than attempt to renew statutory authority, in piecemeal fashion, with temporary statutes such as the EAA.

The political question doctrine poses an obstacle for court challenges. However, the courts should not shy away from

\begin{itemize}
  \item \textsuperscript{353} See discussion \textit{supra} part IV.A.
  \item \textsuperscript{354} The scenarios were (a) an individual distributing an English language analysis of cryptography, (b) source code in print form, (c) source code on floppy disk, (d) posting source code to the Internet, (e) giving a lecture on cryptography and (f) having a conversation about cryptography which reaches a foreign national. See discussion \textit{supra} part IV.A.1.
  \item \textsuperscript{355} See discussion \textit{supra} parts IV.B.2.d, V.B-C.
  \item \textsuperscript{356} See discussion \textit{supra} part IV.C.1.b.
  \item \textsuperscript{357} See discussion \textit{supra} part IV.C.
\end{itemize}
resolving constitutional questions because they relate to foreign policy and national security. The courts should be willing to decide these cases on the merits, as they present novel issues on constitutional rights, which should not be overwhelmed by national security concerns.

Laura M. Pilkington