Georgia State University Law Review

Volume 13
Issue 2 *February 1997*

Article 14

March 2012

Cryptic Controversy: U.S. Government Restrictions on Cryptography Exports and the Plight of Philip Zimmermann

Ronald J. Stay

CRYPTIC CONTROVERSY: U.S. GOVERNMENT RESTRICTIONS ON CRYPTOGRAPHY EXPORTS AND THE PLIGHT OF PHILIP ZIMMERMANN

INTRODUCTION

On November 9, 1994, Philip Zimmermann, a computer software engineer who lives in Boulder, Colorado, passed through customs at Dulles International Airport.[1] Zimmermann was returning from Europe, where he had been invited to speak on issues of public policy.[2] At the airport, a Customs Special Agent diverted Zimmermann from the normal customs process and subjected him to an individualized luggage search and a lengthy interrogation regarding Zimmerman's possible illegal exportation of dangerous munitions.[3] What was the dangerous "weapon" which interested the U.S. Government so much that it would individually interrogate a U.S. citizen? It was computer software.[4]

Specifically, the software in question is called Pretty Good Privacy, or PGP.[5] PGP, created by Zimmermann, is computer software that transforms plain English data from nearly any personal computer into an encoded[6] version that can only be read by its intended recipient.[7] PGP encodes data so well, in fact, that it is used by everyone from Russian freedom fighters to American criminals to maintain the secrecy of their

[1] Letter from Kenneth C. Bass, III, Attorney for Philip Zimmermann, to Homer Williams, Acting Assistant Commissioner, Office of Internal Affairs, United States Customs Service (1994) (available in Georgia State University College of Law Library).

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *Id.*; William M. Bulkeley, *Cipher Probe: Popularity Overseas of Encryption Code Has the U.S. Worried*, WALL ST. J., Apr. 28, 1994, at A1.

[6] The process of encoding data in this manner is generally referred to as the science of "cryptography." Software that encodes data using cryptography, therefore, is referred to as "cryptographic" or "encryption" software. Those who practice the science of cryptology are called "cryptanalysts" or "cryptographers." WEBSTER'S NINTH NEW COLLEGIATE DICTIONARY 312 (1987).

[7] Bulkeley, *supra* note 5.

communications.[8] It is this effectiveness that worries the U.S. Government so much that in 1993 a Federal grand jury in San Jose, California opened a criminal investigation into whether the worldwide distribution of PGP violated United States laws prohibiting the export of powerful cryptographic software.[9]

This Note will examine the constitutionality of United States export controls of cryptographic software, in the context of both the Zimmermann case and other significant cases of the past decade. Section I will first present a concise history of the science of cryptography and its importance to the U.S. Government. Next, Section II will summarize the relevant statutory and regulatory provisions that govern the export of cryptographic software. Sections III and IV will examine the constitutionality of these restrictions from the perspective of the First and Fifth Amendments, respectively. Finally, Section V will discuss whether regulation of cryptographic exports is a non-justiciable "political question" in the context of recent Ninth and Eleventh Circuit cases.

I. History of Cryptography

Cryptography dates back to 405 B.C., when Lysander of Sparta was one of the first military leaders to use encoded messages to communicate with his confederates.[10] For the majority of its history, cryptography was a vital and exclusive tool of governments, not the public.[11] During World War I, British cryptanalysts used a decoded German message, which implored Mexico to ally with Germany against the United States, to convince the United States to enter the war against Germany.[12] Later, in World War II, Allied cryptanalysts cracked the German and Japanese cipher systems, which contributed greatly to the Allied war effort.[13]

With the emergence of advanced computer technology, however, a strong new demand arose for private encryption

[8] *Id.*

[9] John Markoff, *Federal Inquiry on Software Examines Privacy Programs*, N.Y. TIMES, Sept. 21, 1993, at D1.

[10] BRUCE NORMAN, SECRET WARFARE: THE BATTLE OF CODES AND CIPHERS 15 (1973).

[11] *Long Live NSA: Why Congress Wanted to Clip the Agency's Wings*, INFO. L. ALERT: VOORHEES REP., Mar. 25, 1994, at *2 [hereinafter *Long Live NSA*].

[12] NORMAN, *supra* note 10, at 58-60.

[13] DAVID KAHN, KAHN ON CODES: SECRETS OF THE NEW CRYPTOLOGY 56 (1986).

technology.[14] This demand developed the industry known as "public cryptography."[15]

The first and most rudimentary cryptographic systems[16] were referred to as "non-keyed" systems.[17] In these systems, the sender uses a pre-determined algorithm to encode the message, such as substituting each letter in the message with the letter that is three letters higher in the alphabet.[18] For example, A becomes D, B becomes E, and so forth. The drawback to this system is that if a third party determines the algorithm, it becomes a simple matter for that third party to read the encrypted messages.[19]

The next stage of cryptography was "single-key" systems.[20] In a single-key system, encryption and decryption of a message are accomplished by entering a password or "key."[21] The advantage of this system is that so long as the key remains a secret, it is very difficult to decipher.[22] However, since the same key must be passed between the communicating parties to perform the encryption process, it is possible that the key could be revealed to a third party.[23] The current federal standard for data encryption, called DES, is based on single-key cryptography.[24]

The most recent innovation in cryptography, the method utilized in PGP, is "public-key" cryptography.[25] In public-key cryptography, two keys are used: a public key, used to encrypt messages, and a private key, used to decrypt messages.[26] Two

[14] *Long Live NSA, supra* note 11, at *2.

[15] Public cryptography is the development and use of cryptographic technology by private parties, without governmental oversight or assistance. Kenneth J. Pierce, Comment, *Public Cryptography, Arms Export Controls, and the First Amendment: A Need for Legislation*, 17 CORNELL INT'L L.J. 197, 198 n.5 (1984).

[16] The process by which a certain encryption program will encrypt data is often referred to, in mathematical circles, as the "encryption algorithm." Ira S. Rubenstein, *Export Controls on Encryption Software, in* COPING WITH U.S. EXPORT CONTROLS: 1994, at 177, *3 (PLI Com. Law & Practice Course Handbook Series No. 705, 1994).

[17] Jeff Prosise, *How to Keep it a Secret (Data Encryption Methods and How They Work)*, PC MAG., July 1, 1994, at 315.

[18] *Id.*

[19] *Id.*

[20] *Id.* at 316.

[21] *Id.*

[22] *Id.*

[23] Karl L. Barrus, *Pretty Good Privacy—Protecting Your Privacy*, NETWORK COMPUTING, Apr. 1, 1995, at 146.

[24] Prosise, *supra* note 17, at 321.

[25] Barrus, *supra* note 23, at *2.

[26] *Id.* at *1.

advantages of a public-key system are convenience and security. It allows the sender to freely distribute his or her public key so that messages may be readily encrypted and sent, but the sender may keep his or her private key, required to decrypt the messages, totally private and secure.[27]

One of the best public-key algorithms was developed in 1978 by three mathematicians: Ron Rivest, Adi Shamir, and Len Adelman. Known as RSA, this algorithm combines the security of public-key cryptography with "digital signatures," which allows the sender of a message to add an encrypted electronic "signature" that is unforgeable.[28] PGP is based upon the RSA algorithm.[29]

The creation of PGP was a direct result of the federal "key escrow" proposals.[30] Philip Zimmermann, working in Colorado as a computer consultant at the time of the first key escrow proposals, vehemenently disagreed with the idea of key escrow to the point that he decided to create his own public cryptography standard for free distribution.[31]

Zimmermann labored for six months in creating PGP, and when he was finished, he had created a public-key cryptography system that implemented the advanced RSA algorithm in an easy-to-use fashion for any home computer.[32] When it was

[27] *Id.*

[28] *Id.* at *2.

[29] *Id.* at *3.

[30] First proposed in 1990, the key escrow system, which was reincarnated in 1993 as the Clinton Administration's "Clipper Chip" proposal, was the U.S. Government's proposed solution to the tension between data privacy and effective law enforcement. This was a program whereby manufacturers of secure data devices, such as cellular phones, fax machines, and computer modems, would install secure cryptographic systems, based upon a secret algorithm developed by the National Security Agency, in their products. While providing secure data encryption, these systems would have a secret "back door" that would allow law enforcement agencies, upon a court order, to obtain an escrowed "key" to the device, which would allow the agencies to decrypt and monitor the communications. In attempting to make the key escrow system the federal encryption standard, the U.S. Government has engendered widespread outrage among civil libertarians. Sandy Shore, *Feds Target Software Expert Who Developed Code to Encrypt Data—Computers: Among Some Civil Libertarians, Philip Zimmermann Has Achieved a Kind of Cult-hero Status in the Growing Debate Over Electronic-Privacy Issues*, LOS ANGELES TIMES, Aug. 14, 1994, at 2; Bulkeley, *supra* note 5, at A8.

[31] Bulkeley, *supra* note 5, at A8.

[32] *Id.*; Barrus, *supra* note 23, at *2-*3. Note that immediately after PGP was released to the public in 1991, the firm that had initially developed RSA claimed that Zimmermann had used one of their patented encryption algorithms without permission, a claim which Zimmermann disputed at the time. This controversy was

released in 1991, PGP was a milestone in the development of public cryptography.[33] For the first time, military-grade cryptography was available to the public, a level of security so high that even the ultra-secret, code-breaking computers at the National Security Agency could not decipher the encrypted messages.[34]

After its initial release, PGP quickly became "the de facto worldwide standard for encryption of E-mail."[35] Volunteer computer programmers made enhancements to the original PGP program and translated it to work with many different computer systems.[36] A wide variety of people found PGP and its unbreakable code an invaluable tool: human-rights advocates who could not compromise their sources, writers who wished to electronically transmit chapters of books without divulging the contents to the public, and criminals who used PGP to hide sets of books that recorded drug transactions.[37]

PGP was so well-regarded that in mid-1991, soon after its release, one of Zimmermann's friends, who had received one of the initial copies of PGP, placed a copy of PGP on the Internet.[38] After that, it was only a matter of time before computer users all over the world were using PGP to encrypt their most sensitive data.[39] With the worldwide proliferation of PGP, the U.S. Government began to take a serious interest in Phil Zimmermann.

II. U.S. GOVERNMENT REGULATION OF CRYPTOGRAPHIC SOFTWARE

The United States Constitution grants Congress the power to regulate foreign trade.[40] As early as 1954, Congress enacted

eventually settled when distributors of PGP obtained a license to use the RSA algorithm. Bulkeley, *supra* note 5, at A8.

[33] *See* Markoff, *supra* note 9, at D3; Bulkeley, *supra* note 5, at A8.

[34] Bulkeley, *supra* note 5, at A1, A8.

[35] *Subcommittee on Economic Policy, Trade, and the Environment: Hearing on Mass Market Cryptography and Export Controls*, 101st Cong., 2d Sess. (1993) [hereinafter *Hearings*] (statement of Philip Zimmermann, Computer Software Consultant).

[36] Barrus, *supra* note 23, at *2-*3.

[37] Bulkeley, *supra* note 5, at A8.

[38] *Id.* The Internet is a worldwide network of computers, both publicly and privately owned, which are linked together and accessible to the public. Kevin Maney, *It's Big, It's Confusing—So Why All the Fuss?*, USA TODAY, Nov. 13, 1995, at E1.

[39] Bulkeley, *supra* note 5, at A8.

[40] U.S. CONST. art. I, § 8.

legislation to regulate the export of weapons and munitions.[41] The current statutory authority for federal regulation of weapons and munitions exports is the Arms Export Control Act of 1976 (AECA).[42] In it, Congress delegates authority to control the import and export of "defense articles" and "defense services" to the President of the United States "[i]n furtherance of world peace and the security . . . of the United States."[43] The AECA provides for export control with several basic components: (1) items considered to be defense articles subject to export control under AECA shall be placed on the United States Munitions List; (2) creation of a licensing system whereby would-be exporters of items on the U.S. Munitions List must apply to the federal government for an export license; and (3) criminal penalties for violations of the AECA.[44]

The President, in turn, delegated his enforcement authorities under the AECA to the Secretary of State via the International Traffic in Arms Regulations (ITAR).[45] It is the ITAR that provides the practical administrative guidelines under which the export of dangerous munitions, such as cryptographic software, is regulated.[46]

Procedurally, the ITAR specifies the items that are part of the U.S. Munitions List and therefore subject to export control.[47] Items that are eligible for placement on the Munitions List include those items "specifically designed, developed, configured, adapted, or modified for a military application"[48] and which do not have "predominant civil applications."[49] Among the items on the Munitions List are the following:

> [C]ryptographic devices, software, and components specifically designed or modified therefor, including: (1) Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits,

[41] Mutual Security Act of 1954, ch. 937, 68 Stat. 832 (repealed 1976).

[42] 22 U.S.C. § 2778 (1994).

[43] *Id.* § 2778(a)(1).

[44] *Id.* § 2778(a)-(c).

[45] 22 C.F.R. § 120.1 (1995). Note that, pursuant to this regulation, the actual delegation of authority from the President to the Secretary of State was done via Executive Order 11958, as amended (42 Fed. Reg. 4311 (1977)). However, the ITAR provides the pertinent administrative regulations for the purposes of this Note.

[46] 22 C.F.R. § 120.1(a) (1995).

[47] *Id.* § 121.1 (1995).

[48] *Id.* § 120.3(a).

[49] *Id.* § 120.3(a)(i).

> components or software with the capability of maintaining secrecy or confidentiality of information or information systems, except cryptographic equipment and software as follows: [provides exemptions for mass-produced copy-protected software, banking machines, and low-grade cryptographic devices].[50]

A person in the United States cannot export[51] either an item specifically enumerated on the Munitions List or "technical data . . . and defense services . . . related to the defense articles listed in [Category XIII, which contains cryptographic items]"[52] without an export license from the State Department Office of Defense Trade Controls (ODTC).[53] License requests are considered by ODTC on a case-by-case basis.[54]

There are, however, several exceptions to the licensing requirement that could impact the export of cryptographic software such as PGP. The first of these is the public domain exception, which is "driven by First Amendment concerns and represents the government's effort to balance national security controls and protected speech."[55] This exception essentially provides that any information that is generally available to the public is exempt from the ITAR licensing requirement.[56]

[50] *Id.* § 121.1, Category XIII(b).

[51] The ITAR defines "export" in § 120.17 as: "(1) Sending 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 . . . (4) Disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad." *Id.* § 120.17.

[52] *Id.* § 121.1, Category XIII(k). Note that, in sections 120.10(a)(1), (4), the ITAR defines "technical data" as: "(1) Information, other than software . . . which is required for the design development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes . . . blueprints, drawings, photographs, plans, instructions and documentation . . . (4) Software as defined in § 121.8(f) of this subchapter directly related to defense articles." *Id.* § 120.10. "Software," in turn, is defined in § 121.8(f) as: "[including] but . . . not limited to the system functional design, logic flow, algorithms, application programs, operating systems and support software for design, implementation, test, operation, diagnosis and repair." *Id.* § 121.8(f).

[53] *Id.* § 125.2(a).

[54] 22 U.S.C. § 2778(a)(2) (1994).

[55] Rubenstein, *supra* note 16, at *4.

[56] The specific definition of "public domain" in the ITAR is:

> [I]nformation which is published and which is generally accessible or available to the public: (1) Through sales at newsstands and bookstores; (2) Through subscriptions which are available without restriction to any individual . . . (4) At libraries open to the public . . . (6) Through unlimited distribution at a conference, meeting, seminar, trade show or

There are different interpretations as to whether the public domain exception would apply to cryptographic software in the public domain, such as PGP.[57] Resolution of this question turns on the definition one imparts to certain sections of the ITAR. Under one view, shared by many software developers, software is defined as technical data under Section 120.10 of the ITAR, and since technical data in the public domain, such as PGP, is exempt from the ITAR licensing requirements under Section 125.1(a), public domain encryption software would qualify for an exemption from ITAR licensing.[58]

A different result is reached if one looks at the plain regulatory text of the Munitions List and Section 123. All items specifically enumerated on the Munitions List, which includes both cryptographic software and related technical data, require an export license, and the provisions of Section 123 will "trump" the public domain exception under Section 125.1(a).[59] Further, if one interprets the definition of "defense services" under Section 120.9 to include the export of technical data, then Section 124, which controls the export of defense services, would require licensure of any technical data which might appear to fall under the public domain exception of Section 125.1(a).[60]

The AECA provides criminal sanctions for a violation of any section of the ITAR: imprisonment of up to ten years or a fine of up to one million dollars.[61] Philip Zimmermann, creator of PGP, became the target of a federal criminal investigation, potentially subject to criminal sanctions, in 1993.[62] Federal prosecutors are examining whether the indirect transmission of PGP overseas that resulted from its posting on the Internet violated the AECA and ITAR.[63]

> exhibition, generally accessible to the public, in the United States; . . .
> (8) Through fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community.

22 C.F.R. § 120.11(a) (1995).

[57] *See* Rubenstein, *supra* note 16, at *6.

[58] *Id.* at *6, *7.

[59] *Id.* at *7.

[60] *Id.*

[61] 22 U.S.C. § 2778(c) (1994).

[62] Shore, *supra* note 30, at 3.

[63] *See id.* at 1.

III. THE ITAR REGULATIONS AND THE FIRST AMENDMENT

The First Amendment to the U.S. Constitution states that "Congress shall make no law . . . abridging the freedom of speech."[64] Zimmermann's public distribution of PGP was, in all probability, a protected form of speech under the First Amendment, as several decisions of the U.S. Supreme Court indicate.

Although the Court has made clear, in *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.*,[65] that commercial speech does not enjoy the same level of protection as other forms of speech,[66] Zimmermann's conduct in distributing PGP is likely not commercial speech. Zimmermann distributed PGP for free,[67] without profit or advertisement, and did so primarily for political reasons (to protest the unilateral imposition of government cryptography standards).[68]

Therefore, if one were to consider Zimmermann's actions as political or scientific in nature, rather than commercial, the landmark decision of *Miller v. California*[69] offers some guidance. In *Miller*, the Court stated the basic proposition that "[t]he First Amendment protects works which, taken as a whole, have serious . . . political, or scientific value."[70] Further, if one were to consider the distribution of PGP as a scholarly or academic endeavor, then *University of California Regents v. Bakke*[71] would apply. *Bakke* emphasizes that "[a]cademic freedom, though not a specifically enumerated constitutional right, long has been viewed as a special concern of the First Amendment."[72]

Accepting the premise that the distribution of PGP is protected by the First Amendment[73] raises the question of whether the

[64] U.S. CONST. amend. I.

[65] 425 U.S. 748 (1976).

[66] *See id.* at 758-59.

[67] Bulkeley, *supra* note 5, at A1, A8.

[68] *Id.* at A1.

[69] 413 U.S. 15 (1973).

[70] *Id.* at 34.

[71] 438 U.S. 265 (1978).

[72] *Id.* at 312.

[73] In *Bernstein v. United States Dep't of State*, the District Court agreed with this proposition. Analogizing the "expressiveness" of computer programs to that of literary works under copyright laws, the court held that computer source code was protected speech under the First Amendment. 922 F. Supp. 1426, 1436 (N.D. Cal. 1996). *But see generally* United States v. Edler Indus., 579 F.2d 516, 520 (9th Cir. 1978) (faced with a "colorable claim that the First Amendment furnishes a degree of protection for

ITAR regulations and the accompanying licensing system infringe on those protections to an unacceptable degree.[74] In a First Amendment overbreadth analysis, a reviewing court will consider whether an activity that may be constitutionally regulated by the government is done so in a manner that "sweep[s] unnecessarily broadly and thereby invade[s] the area of protected freedoms."[75]

To determine whether the ITAR, in prohibiting the export of public cryptography, sweeps unnecessarily broadly, a court must note that "even though the governmental purpose [is] legitimate and substantial, that purpose cannot be pursued by means that broadly stifle fundamental personal liberties when the end can be more narrowly achieved."[76]

A facial challenge to the ITAR would be unlikely to succeed, as the Court has demonstrated that it is reluctant to strike down a statute on its face when there are a substantial number of situations in which the statute could be constitutionally applied.[77] Here, there is little doubt that the majority of the items on the U.S. Munitions List, such as firearms, aircraft, and missile technology, are of sufficient national security interest to warrant a constitutional constraint on their export.[78] The Court, however, has historically been most willing to apply the overbreadth doctrine to those statutes that affect fundamental First Amendment rights.[79]

[defendant's] dissemination of technological information [in alleged violation of the ITAR]. . . [Ninth Circuit] deem[ed] it unnecessary in this case to resolve the precise scope of that protection").

[74] One could question the ITAR from a First Amendment procedural perspective, claiming that the ITAR licensing system establishes an unconstitutional prior restraint on speech. This issue was addressed in Kenneth J. Pierce, Comment, *Public Cryptography, Arms Export Controls, and The First Amendment: A Need for Legislation*, 17 CORNELL INT'L L.J. 197 (1984). There, the author traced the process of obtaining an ITAR license and concluded that because the AECA did not provide for judicial review of license determinations (see 22 U.S.C. § 2778(h) (1994)), the ITAR did not meet the procedural requirements of a constitutional prior restraint on speech. *Id.* at 218-19. Moreover, Pierce claims that the legislative history of ITAR does not indicate sufficient congressional authorization for a system of prior restraint. *Id.* at 230-31.

[75] NAACP v. Alabama, 377 U.S. 288, 307 (1964).

[76] *Id.* at 307-08 (quoting Shelton v. Tucker, 364 U.S. 479, 488 (1960)).

[77] Parker v. Levy, 417 U.S. 733, 760 (1974).

[78] 22 C.F.R. §§ 121.1, 121.3, 121.9, 121.16 (1995). See *Edler*, 579 F.2d at 520, for the general proposition that these types of items are of sufficient national security interest to constitutionally warrant export controls. "The federal government undeniably possesses the power to regulate the international arms traffic." *Id.*

[79] Michael C. Dorf, *Facial Challenges to State and Federal Statutes*, 46 STAN. L.

One of the first to argue that the ITAR suffered from First Amendment overbreadth was the U.S. Government. Correspondence between the U.S. Attorney General's Office, the U.S. House of Representatives, and the U.S. Senate evinced concerns that the ITAR "extends too broadly into an area of protected First Amendment speech."[80] The Attorney General believed that the ITAR could constitutionally be applied to prohibit exporters from intentionally assisting foreign enterprises in the acquisition of technology or from distributing technical data for the purpose of soliciting sales of a munition.[81] However, he also believed any other application of the ITAR "to restrict the dissemination of technical data by persons who are not directly connected or involved in any way with any foreign conduct that may have dangerous potential for the United States . . . raise[s] serious constitutional problems."[82]

In a 1989 Ninth Circuit case, *United States v. Posey*,[83] the court addressed some of the First Amendment overbreadth issues surrounding arms export controls.[84] The defendant was convicted of violating the Comprehensive Anti-Apartheid Act (CAAA), an ITAR-like statute that prohibited the export of certain munitions to the Republic of South Africa.[85] In his appeal, the defendant claimed his conviction violated the free speech protections of the First Amendment because the items he had exported to South Africa (aircraft technical manuals) were widely available in the United States public domain.[86]

In rejecting the defendant's argument, the court recognized the legitimate government interest in preventing the flow of sensitive military information abroad. The court stated that even though the defense data exported by Posey was, in fact, widely available within the United States public domain, "national security

REV. 235, 261 (1994).

[80] Letter from Theodore B. Olson, Assistant U.S. Attorney General, to Robert A. McConnell, Assistant U.S. Attorney General *1 (Aug. 28, 1984) (available in Georgia State University College of Law Library).

[81] Letter from Robert A. McConnell, Assistant U.S. Attorney General, to Honorable Clement J. Zablocki, U.S. House of Representatives *3, *4 (1983) (available in Georgia State University College of Law Library).

[82] *Id.* at *4.

[83] 864 F.2d 1487 (9th Cir. 1989).

[84] *See id.* at 1496.

[85] *Id.* at 1490. For the text of the CAAA, see 22 U.S.C. § 5067 (1988) (repealed 1993).

[86] *Posey*, 864 F.2d at 1490, 1496.

concerns may be more sharply implicated by the export abroad of military data than by the domestic disclosure of such data."[87]

On its surface, the *Posey* decision may seem to rebut a First Amendment overbreadth argument for the export of public domain cryptographic technology under ITAR, which imposes essentially the same types of export restraints as the CAAA. However, closer examination of both the CAAA and the AECA-ITAR systems reveals a crucial difference between the two. Under the AECA and ITAR, unlike the CAAA, Congress provided a specific exemption from export controls for those articles that are in the public domain.[88] Thus, the narrow First Amendment holding of the court in *Posey* might not be controlling under the situation faced by Philip Zimmermann, where the controlling regulations have a specific public domain exception.

The U.S. District Court recognized the viability of this type of First Amendment overbreadth claim in *Bernstein v. United States Department of State*.[89] There, a developer of cryptographic software sought injunctive relief from the U.S. State Department's enforcement of the ITAR and the AECA, claiming that the export regulations are overbroad under the First Amendment.[90] Despite arguments by the defendant that recent court decisions and legislation sufficiently narrowed the scope of the ITAR so as to place it beyond reach of an overbreadth attack, the court held that the plaintiff presented a colorable constitutional claim.[91] Although an overbreadth attack was described as "strong medicine," it was justified where the statute in question placed obvious sanctions on protected conduct and had the potential to "significantly compromise the protected speech of third parties."[92]

IV. THE ITAR REGULATIONS AND THE FIFTH AMENDMENT

The Fifth Amendment to the U.S. Constitution[93] provides that

[87] *Id.* at 1496-97.

[88] 22 C.F.R. § 125.1(a) (1995).

[89] 922 F. Supp. 1426 (N.D. Cal. 1996).

[90] *Id.* at 1438.

[91] *Id.*

[92] *Id.* at 1438-39.

[93] In analyzing the relevant issues of substantive due process under the Fifth Amendment, which addresses federal government action, much of the case law cited refers to the due process clause of the Fourteenth Amendment, which addresses state governmental action. Although these are separate amendments, the Court has

the Federal government shall not deprive a person of "life, liberty, or property, without due process of law."[94] The term "due process" may refer to either procedural due process, which refers to the guarantees of procedural fairness in the justice system, or substantive due process, which refers to the general proposition that legislation must be fair and reasonable in content and cannot arbitrarily deprive a citizen of life, liberty, or property.[95]

A. Liberty Interest

The concept of "liberty" within the meaning of the Fifth Amendment has been given an expansive reading by the Court.[96] It has been defined to be more than a freedom from physical, bodily restraint, but rather to include numerous other rights "long recognized at common law as essential to the orderly pursuit of happiness by free men."[97] Among the rights long recognized as part of the concept of liberty is the right to pursue one's chosen profession or calling.[98]

Liberty, however, is not a completely unfettered right under the Fifth Amendment. A person's right to liberty, and therefore his right to pursue any lawful vocation, may be subject to reasonable government restraints that are not arbitrarily imposed.[99] In determining whether such restraints are in fact

interpreted the term "liberty" in the same manner under the due process clauses of both the Fifth and Fourteenth Amendments. Therefore, any general propositions relating to liberty and due process of Fourteenth Amendment case law will apply equally to Fifth Amendment situations. Hampton v. Mow Sun Wong, 426 U.S. 88, 100 (1976); Ernest H. Schopler, Annotation, *Supreme Court's Views as to Concept of "Liberty" Under Due Process Clauses of Fifth and Fourteenth Amendments*, 47 L. Ed. 2d 975, 978 n.1 (1977).

[94] U.S. CONST. amend. V.

[95] BLACK'S LAW DICTIONARY 1203, 1429 (6th ed. 1990).

[96] *See* Meyer v. Nebraska, 262 U.S. 390, 399 (1923).

[97] *Id.*

[98] *See, e.g.,* Allgeyer v. Louisiana, 165 U.S. 578, 590 (1897) ("[The] enjoyment . . . of the privilege of pursuing an ordinary calling or trade . . . is an essential part of [one's] rights of liberty and property, as guaranteed by the Fourteenth Amendment.") (quoting Powell v. Pennsylvania, 127 U.S. 678, 684 (1887)); Greene v. McElroy, 360 U.S. 474, 492 (1959) (right to pursue one's chosen profession without undue government interference is protected by the liberty and property concepts of the Fifth Amendment); 16A AM. JUR. 2D *Constitutional Law* § 590, at 517-18 (1964) (right to pursue one's occupation is "one of the most sacred and most valuable rights of a citizen. A person's business, occupation, or calling is 'property' within the meaning of the constitutional provisions as to due process of law").

[99] *Meyer*, 262 U.S. at 399-400; 16A AM. JUR. 2D *Constitutional Law* § 591 (1964),

reasonable and not arbitrarily imposed, the Court will often employ a balancing test that compares the significance of the liberty interest against the relevant governmental interest.[100]

This balancing test is particularly exacting in relation to the right to pursue one's profession, a right that has been deemed "fundamental" by the Court.[101] A court that reviews legislation curtailing the right to pursue one's profession must employ the "strict scrutiny" standard of review: the ends pursued by the legislation must be "compelling" and the legislation must be "narrowly tailored" to meet those ends.[102]

Philip Zimmermann's chosen profession is as a cryptographic software engineer; therefore, a strong argument may be made that by producing and distributing PGP, Zimmermann was pursuing his chosen profession.[103] If this is true, then the AECA and ITAR have, in this case, acted to curtail one of Zimmermann's fundamental rights. Any court that reviews the constitutionality of the ITAR in this situation, therefore, must utilize the strict scrutiny standard of review.

The obvious governmental interest furthered by the AECA and the ITAR is national security, as is plainly stated in the introduction to the AECA.[104] There is no doubt that national security has long been considered by the Court as a compelling governmental interest.[105] The question thus arises whether

and cases cited therein.

[100] Cruzan v. Director, Missouri Dep't of Health, 497 U.S. 261, 279 (1990).

[101] *See* Dent v. West Virginia, 129 U.S. 114, 121-22 (1889); Hampton v. Mow Sun Wong, 426 U.S. 88, 116 (1976); Schware v. Board of Bar Examiners of New Mexico, 353 U.S. 232, 238-39 (1957); *see also* 16A AM. JUR. 2D *Constitutional Law* § 590, at 518 (1964). In examining state or federal statutes for constitutional infirmity, the Court has traditionally used a two-tier analysis. Laws or regulations that effect rights deemed by the Court to be "fundamental" usually fall in areas such as free speech, marriage, sex, child-rearing, and child-bearing. In *Griswold v. Connecticut*, Justice Douglas grouped these rights under the term "penumbras" of privacy, a group of fundamental rights having their origin in the First, Third, Fourth, and Fifth Amendments. 381 U.S. 479, 484 (1965). Laws which curtail a fundamental right will receive a more rigorous review by the Court than those laws that curtail a non-fundamental right, which usually entail economic legislation. *Id.*

[102] JOHN E. NOWAK & RONALD D. ROTUNDA, CONSTITUTIONAL LAW § 11.4, at 371 (4th ed. 1991).

[103] *Hearings, supra* note 35 (statement of Philip Zimmermann).

[104] 22 U.S.C. § 2778(a)(1) (1994).

[105] *See* HAROLD H. KOH, THE NATIONAL SECURITY CONSTITUTION: SHARING POWER AFTER THE IRAN-CONTRA AFFAIR 74 (1990) ("From the very beginning, our Constitution has been obsessed with the idea of national security."); *see also* New York Times Co. v. United States, 403 U.S. 713 (1971). In *New York Times*, where the

there is compelling governmental interest in national security to prohibit the export of public cryptography software such as PGP.

It is a question that requires some historical analysis. In 1954, when the first predecessor to the AECA was passed (the Mutual Security Act),[106] and in 1976, when the AECA was first passed, cryptography was a more sensitive technology than it is today.[107] However, with the advent of widespread personal computer and communications technology, the finest military-grade cryptographic technology is now legally available all over the world.[108] "The genie is out of the bottle," stated the president of a company that legally distributes PGP in the United States; "[t]here's no way anybody can stop the technology."[109]

Indeed, at the 1993 hearings before the U.S. House Subcommittee for Economic Policy, Trade, and the Environment regarding cryptography and export controls, data security experts testified that strong encryption packages are widely available in the public domain, both in the United States and abroad.[110] Most importantly, they noted, there are numerous foreign implementations of DES and other strong cryptographic algorithms developed entirely outside the United States and therefore beyond the jurisdiction of ITAR, which are readily available worldwide.[111] Thus, as a practical matter, at the very

U.S. sought to enjoin petitioner from publishing classified military studies of the Vietnam War (the "Pentagon Papers"), the Court weighed the value to the U.S. government of keeping the studies secret against the substantial infringement upon petitioner's First Amendment right to free expression. *Id.* at 718-19 (Black, J. concurring). The case is significant for this analysis because although the Court recognized the importance of national security as a governmental interest, it determined that such an interest must be compelling indeed to warrant any encroachment upon such sacred and fundamental rights as those of the First Amendment. *Id.* at 731 (White, J. concurring).

[106] Mutual Security Act of 1954, ch. 937, 68 Stat. 832 (repealed 1976).

[107] *See* Pierce, *supra* note 15. Until the late 1970's, cryptography was almost the exclusive province of the government. *Id.* at 199-203. In fact, the largest and most secretive entity in the American intelligence community, the National Security Agency (NSA), concerns itself almost entirely with cryptography. *Id.* at 201. It was the computer revolution of the 1980's which permanently entrenched both the need for and the availability of public cryptography. *Id.* at 199-201.

[108] *See* Lance Hoffman, *SPA Study of Foreign Availability of Cryptography*, SPA NEWS, Mar. 1994, at *2; Bulkeley, *supra* note 5.

[109] Bulkeley, *supra* note 5.

[110] *See Hearings, supra* note 35 (testimonies of Philip Zimmermann, J. Hendren, Ray Ozzie, Stephen Walker, Don Harbert).

[111] *Id.* It is important to note that the argument against a compelling national

least one could make a strong argument that the worldwide availability of such cryptographic power makes it unlikely that there is any compelling governmental interest in regulating the export of software such as PGP.

B. Void for Vagueness

An alternative Fifth Amendment criticism of the ITAR is that it is unconstitutionally vague and thus "void for vagueness."[112] The doctrine of void for vagueness, as with the doctrine of fundamental rights, stems from the due process clause of the Fifth Amendment and states that a statute is unconstitutionally vague when its language is such that reasonable people must necessarily guess as to the meaning of the law.[113] To determine whether a statute is void for vagueness, a reviewing court will usually focus on whether the statute conveys clearly ascertainable standards and provides fair warning as to what type of conduct is prohibited.[114]

This does not mean, however, that a statute must meet impossible standards of definiteness.[115] A statute is not unconstitutionally vague simply because it is stringent, requires the trier of fact to determine reasonableness, or because clearer language could have been used.[116] Moreover, a facially-vague statute may be saved from constitutional infirmity when a court imposes a narrowing construction on the statute.[117] The Court, however, has historically been most willing to invoke the void for vagueness doctrine in those cases that concern fundamental

security interest is *not* the worldwide prevalence of PGP, for if PGP were truly a threat to national security, its worldwide distribution would only serve to further bolster the argument that ITAR controls and Zimmermann's prosecution are necessary to prevent the recurrence of these types of "exports." Rather, it is the fact that foreign developers have already produced and distributed strong cryptographic algorithms, comparable to PGP, in the worldwide public domain. An April 1994 study by the Software Publishers Association supports this claim. Their study determined that there were over two hundred foreign hardware and software products, employing strong cryptographic algorithms similar to DES and PGP, distributed in over twenty different foreign nations. Hoffman, *supra* note 108, at *2.

[112] *EFF Sues to Overturn Cryptography Restrictions*, ELECTRONIC FRONTIER FOUNDATION (News Release), Feb. 21, 1995, at 2 [hereinafter *EFF Sues*].

[113] 16A AM. JUR. 2D *Constitutional Law* § 818, at 988 (1979).

[114] *Id.* at 989-90; Anthony G. Amsterdam, Note, *The Void for Vagueness Doctrine in the Supreme Court*, 109 U. PA. L. REV. 67, 85-86 (1960).

[115] 16A AM. JUR. 2D, *Constitutional Law* § 818, at 989 (1979).

[116] *Id.*

[117] *Id.*

guarantees, such as speech protected under the First Amendment.[118]

Ironically, one of the first parties to raise the question of unconstitutional vagueness of the ITAR was the U.S. Government.[119] In correspondence between the U.S. Justice Department, Attorney General, and the U.S. Senate, legal analysts first expressed concerns in 1984 that the definitions of "technical data" and "export" under the ITAR were unconstitutionally broad under the current interpretation of the ITAR and had not yet received a sufficient narrowing construction from the courts.[120]

Although the ITAR has since been amended to alter some of these definitions,[121] there is still a rational argument to be made that aspects of the definitional elements of ITAR are unconstitutionally vague. One line of argument centers around the ITAR definition of "software"[122] and is aptly illustrated by the so-called "Karn-Schnier case."[123] There, Phil Karn, a telecommunications engineer, applied to the State Department in 1994 for an ITAR export license for two items: a book entitled "Applied Cryptography," which contained detailed computer source program listings[124] for several powerful cryptographic

[118] Amsterdam, *supra* note 114, at 75, 94. "[T]he doctrine of unconstitutional indefiniteness has been used by the Supreme Court almost invariably for the creation of an insulating buffer zone of added protection at the peripheries of several of the Bill of Rights freedoms." *Id.* at 75. "It is evident that the First Amendment freedoms receive most solicitous protection from today's Court." *Id.* at 94.

[119] Memorandum from Larry L. Simms, U.S. Dept. of Justice Office of Legal Counsel to Davis R. Robinson, Legal Adviser U.S. Department of State *15 (Jul. 5, 1984) (available in Georgia State University College of Law Library) ("We remain of the opinion, however, that on their face, the ITAR still present some areas of potentially unconstitutional application, and, moreover, that we cannot be certain whether existing case law would be sufficient to narrow the range of application to a constitutionally sufficient extent.").

[120] *Id.* at *5-*9, *15; Letter from Robert A. McConnell, U.S. Department of Justice, to Honorable Jake Garn, U.S. Senate *4 (1984) ("[We] concluded that the [ITAR] applied a prior restraint . . . to a wide variety of protected speech. . . . [S]uch speech would generally be protected by the First Amendment. . . . Our experience with . . . the ITAR, however, cause us concern that the task of narrowing this type of statutory scheme by regulation is formidable.") (available in Georgia State University College of Law Library).

[121] 58 Fed. Reg. 39,280 (1993). These amendments altered the definitions of "technical data," "expert," and "public domain." *Id.*

[122] Rubenstein, *supra* note 16, at *6-*7.

[123] *Id.* at *13-*14.

[124] "Source program" refers to the actual computer programming instructions that one may enter into a computer to enable it to perform a given function. RICHARD

algorithms, and a source disk, which contained the same source program as the book, but in magnetic form.[125] Karn was granted the license for export of the book, but denied a license for export of the disk on the grounds that the disk was a munition within the meaning of the ITAR.[126]

In a separate incident, a California resident, Daniel Bernstein, sued the U.S. State Department in 1995 after it determined that Bernstein would need an ITAR export license to publish a scientific paper containing the source program for an encryption program.[127] Critics view conflicts like these as evidence that the ITAR restrictions are overly vague.[128] John Gilmore, the cofounder of the Electronic Frontier Foundation[129] stated:

> There's a whole continuum [sic] between a book about cryptography, a book listing source code, an on-line copy of that book, a piece of actual source code, a piece of binary code stored on diskette, a piece of binary code loaded into a general-purpose computer, and a machine that does nothing but encoding and decoding. Somewhere along that continuum [sic], you go from having full rights to anything you want, to having no export rights. It's not clear where the line should be drawn.[130]

In his practitioner's analysis of the ITAR, Ira Rubenstein notes the vague interplay between the definitions of software, technical data, and public domain under the ITAR.[131] He notes that although books about cryptography should be exportable under the public domain exception, it is not clear whether books published in an "on-line" format or with a source program

HIPGRAVE, COMPUTING TERMS AND ACRONYMS: A DICTIONARY 101 (1985).

[125] *Crypto Speech Case Heating Up: Software Engineer Threatens to Sue State Dept. Over Blocked Attempt To Export A Disk*, INFO. L. ALERT: VOORHEES REP., Dec. 9, 1994, at *1.

[126] *See id.*

[127] *Export Control Case Exposes Conflict Between Speech and Security: Challenge Of Law Governing Shipping Cryptography Overseas May Be In For Rough Time In Federal Court*, INFO. L. ALERT: VOORHEES REP., Mar. 10, 1995, at *1. Bernstein's suit later survived the U.S. Government's motion to dismiss, with the court holding that Bernstein presented a colorable Fifth Amendment void-for-vagueness claim. *Bernstein*, 922 F. Supp. at 1439.

[128] *EFF Sues*, *supra* note 112, at 1-2.

[129] The Electronic Frontier Foundation (EFF) is a non-profit group which advocates civil liberties in electronic media, such as computers. Rubenstein, *supra* note 16, at *122 n.50.

[130] *Id.* at *13.

[131] *Id.* at *13-*16.

diskette attached would fall under the software[132] definition, the published work[133] definition, or even the technical data[134] definition.[135]

In the past, however, federal courts have attempted to narrow the vague provisions of the ITAR. In *United States v. Edler Industries*,[136] the Ninth Circuit addressed the overly-broad definition of "technical data" under the predecessor regulations to the ITAR,[137] stating that the definition was "susceptible of an overbroad interpretation. . . . A broad statutory reading, however, is neither necessary nor proper. In our opinion, technical data must relate in a significant fashion to some item on the Munitions List."[138]

The defendant in *Edler* was exporting technical data related to missile production, and while the court's narrowing interpretation that technical data must *significantly* relate to an item on the Munitions List, was sufficient to alleviate the immediate controversy in that case,[139] it may not have significant impact on the PGP export situation. Although the current version of the ITAR recognizes that technical data must relate to items on the Munitions List to be subject to export restrictions[140] (the narrowing construction in *Edler*), the *Edler* ruling does not seem to resolve any potential vagueness in the current ITAR's definition of technical data and its relationship to software.

Philip Zimmermann has raised the additional issue of the potentially far-reaching meaning of "export" under the ITAR.[141] Under the expansive definition of export under Section 120.17(a)

[132] *See supra* note 52 (defining "software" under the ITAR).

[133] *See supra* note 56 (defining published works, which fall under the "public domain" exception to the ITAR).

[134] *See supra* note 52 (defining "technical data" under the ITAR).

[135] Rubenstein, *supra* note 16, at *13-*14. Note that Rubenstein's question here is premised upon interpretation of yet another vague provision of the ITAR: whether public domain encryption software is subject to the public domain exception in § 125.1 of the ITAR. Before even reaching the question of the definitional vagueness of software, Rubenstein assumed that public domain cryptographic software and technical data are not subject to the public domain exception of the ITAR. *See generally id.* at *6-*7.

[136] 579 F.2d 516 (9th Cir. 1978).

[137] Mutual Security Act of 1954, ch. 937, 68 Stat. 832 (repealed 1976).

[138] 579 F.2d at 520.

[139] *Id.* at 518, 520-21.

[140] 22 C.F.R. §§ 120.10(a)(1), 121.1 Category XIII(k), 125.1(a) (1995).

[141] *Hearings*, *supra* note 35 (statement of Philip Zimmermann).

of the ITAR,[142] a Boeing executive who carries his notebook computer to the Paris airshow and sends a PGP-encrypted electronic mail message to his office in Seattle (without first obtaining an export license) would be in violation of the ITAR and subject to criminal sanctions.[143] Yet, it seems doubtful that a reasonable person would interpret the ITAR to prohibit this type of behavior.

V. The United States Munitions List as a Political Question

Despite the potential validity of any First or Fifth Amendment attack on the constitutionality of the ITAR licensing scheme for public cryptography, a 1990 Eleventh Circuit decision may render all these arguments moot. In *United States v. Martinez*,[144] the court reviewed the appellants' conviction, under AECA and ITAR, for the export of "Videocipher II," a piece of cryptographic hardware that is a defense article subject to ITAR export restrictions.[145]

Appellants' defense, similar to a potential defense for the export of PGP, rested upon a First Amendment overbreadth argument.[146] They claimed that the inclusion of cryptographic devices on the United States Munitions List was "overbroad because [the general heading of cryptographic devices and software] includes items already in the public domain whose dissemination would pose no security threat, and which lack any characteristic that is inherently or predominantly military."[147]

In rejecting this defense, the court held that placement of items on the Munitions List was a political question, and therefore excluded from judicial review.[148] The court cited three reasons to support this conclusion: (1) a lack of judicially manageable standards to determine whether the cryptographic item belonged on the Munitions List, (2) the court's lack of access to the classified intelligence reports upon which placement decisions are made, and (3) recent congressional amendments to

[142] *See supra* note 51 (defining "export" under the ITAR).

[143] *Hearings, supra* note 35 (statement of Philip Zimmermann).

[144] 904 F.2d 601 (11th Cir. 1990).

[145] *Id.*

[146] *Id.* A potential First Amendment overbreadth argument for the free distribution of PGP is addressed *supra*, Section III of this Note.

[147] *Id.*

[148] *Id.* at 602.

the AECA which precluded judicial review of the Munitions List.[149]

The political question doctrine, upon which the *Martinez* court based its decision, traces its origins to the landmark 1849 decision in *Luther v. Borden.*[150] There, in the context of a dispute over Article IV of the U.S. Constitution and the legitimacy of the government of Rhode Island, Chief Justice Taney determined that interference in certain domestic concerns of a state are political in nature and, therefore, cannot be reviewed by the judicial branch.[151]

Although the exact boundaries of the political question doctrine are unclear, it has, subsequent to *Luther*, been applied in several areas, including foreign affairs, amendments to the Constitution, the Guaranty Clause, and political gerrymandering.[152] In an attempt to delineate a somewhat nebulous concept, one commentator identified three important components of this doctrine: (1) the Court, due to lack of information, cannot fully clarify the relevant questions involved, (2) the Court will defer to the constitutionally proper decisions of another branch, and (3) the Court will defer to the wider responsibilities of the elected branches.[153]

The placement of cryptographic software such as PGP on the U.S. Munitions List could be a non-justiciable political question under the *Martinez* rationale. Much of the information regarding the security threat of cryptographic software is classified and not available to the courts,[154] and both the President and Congress are well within their constitutional authority in regulating the export of munitions.[155]

However, one commentator has rejected the use of the political question doctrine to preclude judicial review in the area of foreign affairs.[156] In his thorough examination of the Constitution and national security, Harold Koh asserts that the three traditional arguments supporting the non-justiciability of

[149] *Id.* at 602-03.

[150] 48 U.S. 1 (1849).

[151] *Id.* at 42.

[152] NOWAK & ROTUNDA, *supra* note 102, § 2.15, at 108-12.

[153] *Id.* at 114.

[154] *Martinez*, 904 F.2d at 602.

[155] See discussion of Congressional and Presidential authority to regulate arms exports, *supra* Section II of this Note.

[156] KOH, *supra* note 105, at 220-24.

foreign affairs issues lack merit. They are: an inability to derive principled standards, the informational inability of the judiciary to make foreign affairs decisions, and separation of powers issues.[157] He further states that the courts have "excluded themselves too thoroughly from the national security area"[158] and that a "rich historical tradition of judicial decision making in foreign affairs,"[159] as well as principles of federalism, require the judiciary to assume a more active role in national security and foreign affairs decisionmaking.[160]

This line of reasoning is further supported by the nature of the rights involved in a prohibition of the export of PGP. Adjudging PGP's export control a political question would run afoul of the Supreme Court's general unwillingness to apply the political question doctrine to issues when individual liberties, protected by the Bill of Rights, are implemented.[161]

The *Bernstein* court agreed with this reasoning.[162] In an opinion upholding the justiciability of the plaintiff's claim that cryptographic software should not be included on the U.S. Munitions List, the court did not dispute that the plain language of the AECA precluded judicial review of commodity jurisdiction determinations.[163] However, the plaintiff's claim was best described as a constitutional challenge to a federal statute, not a review of a specific commodity jurisdiction decision.[164] Therefore, this constitutional question was best resolved by the judicial branch.[165]

CONCLUSION

Regardless of the merits of any potential constitutional argument against the validity of the ITAR and its application to the Zimmermann case, it is uncontroverted that Zimmermann's situation and the similar situations of others have engendered diverse opposition to the ITAR.[166] Bills have been introduced in

[157] *Id.* at 221-22.

[158] *Id.* at 183.

[159] *Id.* at 220.

[160] *Id.* at 223-24.

[161] *Id.* at 220; NOWAK & ROTUNDA, *supra* note 102, § 2.15, at 114.

[162] 922 F. Supp. at 1431-36.

[163] *Id.* at 1431.

[164] *Id.*

[165] *Id.*

[166] Bulkeley, *supra* note 5, at A8.

Congress to relax the ITAR export restrictions on cryptographic software.[167] Even the late Ron Brown, former U.S. Secretary of Commerce, urged that the United States ease the ITAR export controls on cryptographic software.[168]

Further, in direct response to the Zimmermann and *Bernstein* cases, the Electronic Frontier Foundation (EFF) sponsored a lawsuit in early 1995, seeking to restrict the federal government from regulating cryptographic exports.[169] The EFF suit claimed that the ITAR, as applied to cryptography, was in violation of both the First and Fifth Amendments.[170]

Perhaps the best indication of the legal infirmity of the U.S. Government's restriction of cryptographic exports is the federal government's own resolution of the Philip Zimmermann investigation. In January, 1996, the U.S. Attorney responsible for the criminal investigation of Zimmermann announced that the government had decided to drop the prosecution and not seek an indictment.[171] No reason was given for the decision.[172]

A professor of law has stated that the right to "speak" cryptographically is protected by the U.S. Constitution as much as "the right to speak Navajo. . . . The government has no particular right to prevent [someone] from speaking in a technological manner even if it is inconvenient for them to understand."[173] It is therefore essential that any governmental restraints on rights as fundamental as free speech or the right to practice one's chosen profession advance a compelling

[167] In 1993, Representative Maria Cantwell of Washington introduced a bill to the U.S. House of Representatives that would have relaxed the ITAR export restrictions. John Schwartz, *Bill Would Ease Curbs on Encoding Software Exports*, WASH. POST, Nov. 23, 1993, at C1. The bill did not pass, but it may have impacted the 1993 amendments to the ITAR that liberalized the export controls on mass-market software products with cryptographic ability. *See* 58 Fed. Reg. 39,290 (July 22, 1993).

A similar bill was introduced to the U.S. Senate in 1996 by Senator Conrad Burns of Montana and to the U.S. House of Representatives by Representative Bob Goodlatte of Virginia. Scott Ritter, *Congress Urged to Lift Ban On Data Encryption Exports*, DOW JONES INT'L NEWS, June 26, 1996.

[168] Dinah Zeiger, *Brown to Urge Easing Export Controls on Encryption Software*, DENVER POST, Jan. 13, 1996, at E1.

[169] *EFF Sues, supra* note 112, at 1.

[170] *Id.* at 2.

[171] Elizabeth Weise, *Privacy Software Writer Won't Be Prosecuted*, ATLANTA J. & CONST., Jan. 16, 1996, at D6.

[172] *Id.*

[173] Markoff, *supra* note 9, at D3 (quoting Professor Eben Moglen, Columbia University School of Law).

governmental interest in a narrowly tailored fashion. The ITAR, however, may not advance such a compelling interest, given the worldwide proliferation of good cryptographic software in the public domain. In addition, the ITAR definitions have not kept up with the rapid changes in computer technology, and therefore may not give sufficient notice of the type of conduct that is prohibited under the ITAR, which lends support to an argument that the ITAR is unconstitutionally vague.

Ronald J. Stay