University of Chicago Legal Forum

Volume 1996 | Issue 1 Article 15

Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation

Adam C. Bonin
Adam.Bonin@chicagounbound.edu

Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation

Adam C. Bonin†

We live in an age in which the state gradually has eroded the right to privacy. Whether sexual practices[1], searches of one's garbage bags,[2] or random drug testing in high schools[3] is the issue, courts have given the government increased freedom to examine and explore areas of life which many believe are shielded from public scrutiny. "[A]sk anyone and they will tell you that they have a fundamental right to privacy. They will also tell you that privacy is under siege."[4]

Given this erosion of privacy, it is no surprise these issues also exist in cyberspace. For many users of the Internet, data encryption programs[5] represent the sole means to protect their messages from outsiders, including the government.[6] Even though the reasons why a third party, particularly the government, might take interest in reading their messages rarely are articulated, the sentiment remains quite strong.[7] If I take the

---

† B.A. 1994, Amherst College; J.D. Candidate 1997, University of Chicago.

[1] *Bowers v Hardwick*, 478 US 186 (1986).

[2] *California v Greenwood*, 486 US 35 (1988).

[3] *Vernonia School District v Acton*, 115 S Ct 2386 (1995).

[4] Ellen Alderman and Caroline Kennedy, *The Right To Privacy* xiii (Knopf, 1995). For example, in a Time/CNN poll of 1,000 Americans conducted in 1994 by Yankelovich Partners, two-thirds of Americans "said it was more important to protect the privacy of phone calls than to preserve the ability of police to conduct wiretaps. When informed about the Clipper Chip, 80% said they opposed it." Philip Elmer-Dewitt, *Who Should Keep the Keys*, Time 90 (Mar 4, 1994).

[5] Data encryption programs seek to hide data by using mathematical formulae to translate plain English into a format in which only the owner of the document can read. The technology behind encryption software is described in Part I.

[6] See, for example, John Perry Barlow, *The Denning-Barlow Clipper Chip Debate*, http://www.eff.org/papers/barlow-denning.html (Mar 10, 1994) ("Everytime [sic] we make any sort of transaction in a digital environment, we smear our fingerprints all over Cyberspace. If we are to have any privacy in the future, we will need virtual 'walls' made of cryptography.").

[7] See, for example, Eric Hughes, *A Cypherpunk's Manifesto*, http://weber.u.washington.edu/~phantom/cpunk/cpunk.manifesto (Mar 3, 1993) ("Privacy in an open society also requires cryptography. If I say something, I want it heard only by those for whom I intend it. If the content of my speech is available to the world, I have no

extra steps to encrypt my documents, the argument goes, then what right do others have to force me to reveal what I have written?

There remains another story to tell. For the law enforcement community, data encryption poses a serious threat to the ability to detect and punish crime.[8] Problems range from decrypting child pornography files hidden on a user's hard drive to determining whether a PGP-encoded message between a military officer and foreign contacts represents attempted espionage.[9] While phone wiretaps and other current detection methods provide the evidence in a comprehensible form, encryption technology allows comprehension to only a privileged few—those who hold the keys. Unlike a safe which others can crack or a foreign language which experts can translate, current encryption technology stands virtually impenetrable, allowing easy, completely secure transfer and retention of any document.[10] Indeed, rampant use of data encryption by foreign enemies could threaten national security if our government cannot crack the codes of foreign powers as it did during World War II.[11]

---

privacy.").

[8] In announcing the President's initiative to develop "Clipper Chip" technology, the Press Secretary noted that encryption technology "helps to protect the privacy of individuals and industry, but it also can shield criminals and terrorists." *Statement of the Press Secretary*, http://bilbo.isu.edu/security/isl/clipper.html (Apr 16, 1993).

[9] According to FBI Director Louis Freeh, the FBI has encountered encryption technology being used by child pornographers and Filipino terrorists who planned the assasination of Pope John Paul II. In addition, Professor Dorothy Denning of Georgetown University has surveyed law enforcement agencies regarding the use of encryption technology in furthering crimes: "'I came up with over 20 cases—child pornography, terrorism, murder, embezzlement, fraud, tax protestors, export violations—and, in some cases, they were able to crack it, and others they couldn't.'" Peter H. Lewis, *The FBI Sting Operation on Child Pornography Raises Questions About Encryption*, New York Times D5 (Sept. 25, 1995).

[10] James K. Kallstrom, who is an FBI Special Agent stated:

> The essence of the cryptographic threat is that high-grade and user-friendly encryption products can seriously hinder law enforcement and counterintelligence agencies in their ability to conduct electronic surveillance that is often necessary to carrying out their statutorily-based missions and responsibilities. . . . Real-time decryption is often essential so that law enforcement can rapidly respond to criminal activity and, in many instances, prevent serious and life-threatening criminal acts.

Communications and Computer Surveillance, Privacy and Security, Hearing before the Subcommittee on Technology, Environment and Aviation of the House Committee on Science, Space, and Technology, 103rd Cong, 2d Sess 25 (1994).

[11] See John Keegan, *The Second World War* 496-502 (Penguin, 1989).

This Comment begins with background information on the nature of cryptography and an explanation of how modern public-key cryptography software functions. It surveys the state of the law regarding cryptography and current restrictions on the export of cryptographic software. It then considers the question of cryptography and the First Amendment. This Comment then argues that encrypted documents represent a form of speech, and as such, should receive protection by the First Amendment from a ban on their use. Precedent suggests that the courts will not accept "national security" or "the needs of law enforcement" as sufficient justifications to ban innocent cryptography usage.[12]

Given that the government cannot ban cryptography, this Comment finally argues that the Fifth Amendment precludes the government's ability to coerce individuals to decrypt their documents. As long as users memorize their passwords and do not commit them to paper, the government will prove unable to force them to decrypt their documents. The Fifth Amendment privilege against self-incrimination acts as a shield against such attempts.

I. ENCRYPTION AND THE INTERNET

As legend has it, cryptography started with Julius Caesar. Not trusting his messengers to keep his missives private, he shifted every letter in a document a fixed amount, for example turning A's into D's, B's into E's, and so forth. Only those whom Caesar entrusted with the knowledge of the rotation scheme could understand his messages, allowing him to send detailed military directives to the front in confidence. Since that time, governments and private citizens have turned to increasingly complex means of recording information, using mathematical formulae generated by computers. These programs, far more elaborate than the Caesarian rotation system, can assure the sender that only the intended recipient can decipher the document and read its contents.[13]

Public-key encryption overcomes the inherent difficulty in other encryption schemes. Prior methods required the sender to first transmit the encryption scheme through nonsecure channels so that the recipient would know how to decrypt the actual documents. The old system remained inherently flawed because com-

---

[12] See Part III.B.2.

[13] This story and others, including the development of cryptography in America by such people as Thomas Jefferson, can be found on the Internet. See *Cryptography Timeline*, http://www.clark.net/pub/cme/html/timeline.html (June 2, 1996).

munications could not begin without first risking the safety of the code as the deciphering mechanism itself could not be sent encrypted. In 1976, Whitfield Diffie and Martin Hellman published a paper titled *New Directions in Cryptography*, outlining how a concept called "public key" encryption could overcome the difficulty.[14]

A public-key system generates two related password keys, one "public" and one "private"; each key consists of a randomly generated string of alphanumeric characters.[15] The user makes her public key known to those who want to send her secure messages. Those people use that key to encrypt messages sent to her. To decrypt those messages requires the use of the private key, which only the owner possesses.[16] Complete strangers can use public-key encryption systems with the assurance that their messages remain confidential. Currently, there exists no verified way to determine the private decoding key by looking at the public encoding key.[17]

On the Internet, a public-key encryption program called Pretty Good Privacy ("PGP") has become the de facto standard.[18]

---

[14] Whitfield Diffie and Martin E. Hellman, *New Directions in Cryptography*, IT-22 IEEE Transactions on Information Theory 644 (1976).

[15] For example, this is the PGP public key of Sen. Patrick Leahy of Vermont:

```
---BEGIN PGP SIGNATURE--- Version: 2.6.2
iQCVAwUBMYjdVBM5YGSLu9/1AQGFwwQArk/HYG65cSOr3dsykvkDFonjISju
r7xbSEMCFLI3E4KSoXSy4 6cNogICGADxDnwI8j/29Gviu d93eQ2veeNmKP43
r0R Zcv86b3/pK6btq3QqVN6 x3G8CEA2MnDtuSWbNyANEdValtpOYTCzU2Sm
6gNfg9Q 4QxUZ4R4 Ps= =VJ87
-----END PGP SIGNATURE-----
```

Senator Leahy published his key as an attachment to a letter sent out on behalf of pro-cryptography legislation he was sponsoring. See *Letter from Senator Patrick Leahy (D-VT) on Encryption*, http://www.eff.org/pub/Privacy/Key_escrow/Crypto_bills_1996/leahy_pgp_960502_net.letter (May 2, 1996).

[16] One analogy might be as follows: If I want people to call me on the telephone, I give them my phone number, and those digits must be entered before someone can call me. At the same time, I am the only one posessing the phone equipment that can answer a call placed to that number. In order to listen to my phone calls, one needs to break into my house or tap into the line before the communication enters my house. A good public key system constructs an impenetrable fortress on both fronts.

[17] From the *PGP Frequently Asked Questions With Answers* 1.3, http://www.cis.ohio-state.edu/hypertext/faq/usenet/pgp-faq/part1/faq.html (June 22, 1995).

[18] Steven Levy, *The Cypherpunks vs. Uncle Sam*, New York Times Magazine 44, 60 (June 12, 1994). PGP is based on the RSA mathematical encryption formula, which works as follows:

1. Find P and Q, two large (e.g., 1024-bit) prime numbers.
2. Choose E such that E and (P-1)(Q-1) are *relatively prime*, which means they

Because of the relative ease of use of its interface, many in the Internet community consider PGP to offer a radically democratizing tool, allowing all citizens to have a level of privacy previously enjoyed by an elite few.[19] Encryption technology thus could upset the balance between the state and the individual and make it impossible for law enforcement agencies to conduct investigations in cyberspace. According to Phil Zimmerman, author of Pretty Good Privacy:

> If privacy is outlawed, only outlaws will have privacy. Intelligence agencies have access to good cryptographic technology. So do the big arms and drug traffickers. So do defense contractors, oil companies, and other corporate giants. But ordinary people and grassroots political organizations mostly have not had access to affordable military grade public-key cryptographic technology. Until now. PGP empowers people to take their privacy into their own hands. There's a growing social need for it. That's why I wrote it.[20]

A recently published scientific paper has raised the first doubts about the impenetrability of public-key systems.[21]

---

have no prime factors in common. E does not have to be prime, but it must be odd. (P-1)(Q-1) can't be prime because it's an even number.
3. Compute D such that (DE-1) is evenly divisible by (P-1)(Q-1). Mathematicians write this as DE = 1 mod (P-1)(Q-1), and they call D the *multiplicative inverse* of E.
4. The encryption function is *encrypt*(T) = (T^E) *mod* PQ, where T is the plaintext (a positive integer) and "^" indicates exponentiation.
5. The decryption function is decrypt(C) = (C^D) *mod* PQ, where C is the ciphertext (a positive integer) and "^" indicates exponentiation.
Your *public key* is the pair (PQ, E). Your *private key* is the number D (reveal it to no one). The product PQ is the *modulus*. E is the *public exponent*. D is the *secret exponent*.
You can publish your public key freely, because there are no known easy methods of calculating D, P, or Q given only (PQ, E) (your public key). If P and Q are each 1024 bits long, the sun will burn out before the most powerful computers presently in existence can factor your modulus into P and Q.

The Mathematical Guts of RSA Encryption, http://www.ai-lab.fh-furtwangen.de/~dziadzka/Vortraege/Cryptography/the_mathematical_guts_of_rsa_encryption.html. There are no export restrictions on publishing the mathematical formulae; only the dissemination of means of implementation are barred. For a description of how PGP works as a user interface see *EFH Pretty Good Privacy Workshop*, http://www.efh.org/pgp/pgpwork.html#ufriend (Jan 14, 1995).

[19] Phil Zimmerman, *Why Do You Need PGP?*, http://www.math.ucla.edu/pgp/volume1/WhyDoYouNeedPGP.html (Sept 8, 1994).

[20] Id.

[21] Paul C. Kocher, *Cryptanalysis of Diffie-Hellman, RSA, DSS, and Other Systems*

Cryptanalyst Paul Kocher explained that attackers could use outside measurements of the time used to complete cryptographic operations to determine how the keys are generated. With that information, a skilled hacker could have an easier time determining the keys themselves.[22] While not yet attempted in practice, Kocher's theory of using timing attacks presents the first substantial challenge to the reliability of PGP.[23]

II. THE LAW'S TREATMENT OF ENCRYPTION

According to the United States Government, Phil Zimmerman, designer of PGP and a winner of a Chrysler Innovation in Design Award, may also be an arms trafficker and international munitions dealer. Under the Arms Export Control Act[24] and the International Traffic in Arms Regulations ("ITAR"),[25] cryptographic software represents a dangerous munition which people cannot export from the United States. Because Zimmerman placed PGP on the Internet for public access and downloading, one could argue that he knowingly allowed its export around the world in violation of the Act. The government convened a grand jury against Zimmerman to determine whether he violated ITAR. On January 11, 1996, the government announced that it would not file charges against Zimmerman, but made no statement whether others might suffer under ITAR in the future.[26]

Using Timing Attacks, http://www.cryptography.com (Dec 7, 1995). One hint of the importance of Kocher's work is the fact that the New York Times ran a front-page article of Kocher's work after his abstract was first released. John Markoff, *Secure Digital Transactions Just Got a Little Less Secure*, New York Times A1 (Dec 11, 1995).

[22] Markoff, New York Times at A1 (cited in note 21).

[23] Id. The security of PGP is premised on the notion that outsiders cannot determine the prime numbers used in its key generation. A successful timing attack would give the potential code cracker a good start in determining how they were generated, thus reducing the search for the keys to a more manageable size.

Even if timing attacks can be used to foil PGP, there will doubtless be conceived other cryptographic methods immune to timing attacks whose decryption would require the owner to reveal the password. As such, neither Kocher's article nor other challenges to PGP moot the analytical thrust of this Comment.

[24] 22 USC § 2778 (1996).

[25] 22 CFR § 121.1, Category XIII(b)(1) (1995).

[26] Elizabeth Corcoran, *U.S. Closes Investigation In Computer Privacy Case*, Washington Post A11 (Jan 12, 1996). Word spread quickly on Usenet discussion groups such as alt.security.pgp and talk.politics.crypto when the announcement was made, including an acknowledgement of thanks by Zimmerman himself. A copy of the Justice Department's press release may be found on the World-Wide Web on the home page for the Center for Democracy and Technology, a computer civil-liberties organization. See http://www.cdt.org/crypto/zimm_1_11_pr.html.

The Arms Export Control Act empowers the President, with the advice of the Director of the Arms Control and Disarmament Agency, to designate as nonexportable those items which would "contribute to an arms race, aid in the development of weapons of mass destruction, support international terrorism, increase the possibility of outbreak or escalation of conflict, or prejudice the development of bilateral or multilateral arms control or nonproliferation agreements or other arrangements."[27] The United States Munitions List[28], which lists all devices and material prohibited from export, bans cryptographic methods by which users secure data.[29]

The inclusion of cryptographic software on the United States Munitions List is not subject to judicial review. In *United States v Martinez*,[30] producers challenged the placement of video descrambling units on the list. These units were classified under the same Category XIII(b) list of data-altering devices as cryptographic software. Judge Roney, writing for the court, held that the courts had no standing to adjudicate the issue. The "political question" doctrine governed these decisions, and only the more democratically responsive branches of government could make these determinations:

> The consequences of uninformed judicial action could be grave. Questions concerning what perils our nation might face at some future time and how best to guard against those perils "are delicate, complex, and involve

---

[27] 22 USC § 2778(a)(2) (1995).

[28] 22 CFR § 121.1 (1995).

[29] The relevant section includes:

> Information Security Systems and equipment, cryptographic devices, software, and components specifically designed or modified therefore, including:
>
> (1) Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems, except cryptographic equipment and software as follows:
>
> (i) Restricted to decryption functions specifically designed to allow the execution of copy protected software, provided the decryption functions are not user-accessible.
>
> (ii) Specially designed, developed or modified for use in machines for banking or money transactions, and restricted to use only in such transactions. Machines for banking or money transactions include automatic teller machines . . . .

22 CFR § 121.1, Category XIII(b) (1995).

[30] 904 F2d 601 (11th Cir 1990).

> large elements of prophecy. They are and should be undertaken only by those directly responsible to the people whose welfare they advance or imperil. They are decisions of a kind for which the Judiciary has neither aptitude, facilities nor responsibility and which has long been held to belong in the domain of political power not subject to judicial intrusion or inquiry."[31]

Regardless of any restrictions on the export of encryption software, PGP and similar software have quickly reached across the world via the Internet and the World-Wide Web.[32] Even if one erased all the copies currently extant, both foreign and domestic cryptographers could replicate the software algorithms or create good facsimiles fairly quickly. The aphorism that national borders have been mere speed bumps on the information superhighway[33] seems true; once in cyberspace, encryption technology spreads uncontrollably.

III. LEGAL CONSTRAINTS UPON POTENTIAL ENCRYPTION REGULATION

A. Technology Has Outpaced Law Enforcement And Regulating The Strength of Encryption Technology Would Prove Unwise

Data encryption by private citizens would not present an obstacle for the government if it could access the "plaintext" of communications without the owner's assistance or knowledge.[34] Few safes owned by private citizens remain so secure that the government cannot forcibly open them when necessary. No outsider, however, can "crack open" documents encrypted with the

---

[31] Id at 602. To see other cases in which the courts passed judgment on controversies deemed "political questions," see *Dalton v Specter*, 114 S Ct 1719, 1721 (1994) (refusing to review decision by President Clinton to close the Philadelphia Naval Yard upon challenge by United States Senator Arlen Specter); and *Nixon v United States*, 506 US 224 (1993) (refusing to review Senate procedures during impeachment of District Court Judge Walter Nixon).

[32] Zimmerman has received word that PGP was being taught to refuseniks in the former Soviet Union and Burmese freedom fighters in jungle training camps using laptop computers. According to one letter he received from Latvia, "'Let it never be, but if dictatorship takes over Russia, your PGP is widespread from Baltic to Far East now and will help democratic people if necessary.'" Steven Levy, *The Cypherpunks vs. Uncle Sam*, New York Times Magazine 44, 60 (June 12, 1994) (cited in note 18).

[33] Timothy May, former Intel physicist and co-founder of the "cypherpunk" movement, confirms that he originated this expression (e-mail on file with *University of Chicago Legal Forum*).

[34] By "plaintext," I refer to the original document created by the user, able to be read by other individuals. The encrypted document can be referred to as "ciphertext."

software currently used by computer users. Modern technology now offers citizens the ability to communicate and interact with privacy and security, unlike telephonic communications which the government may legally wiretap.[35]

Two constraints, technological and constitutional, force the resolution of the issue. For the purposes of this paper, the technological constraint is assumed: government computers and cryptanalysts lack the technical knowledge and capacity to decrypt documents encoded with public-key cryptography. Kocher's theory of timing attacks has yet to be implemented.[36] A 1024-bit code (equivalent to 64 characters) would require 2^{1024} keys to be tested in a brute-force attack.[37] A computer processing one million keys per second would take approximately 8.96 times 10^{27} years to complete. The universe is only around 10^{10} years old, by comparison.[38]

In order to disable encryption software's potentially perilous consequences, the government has begun to explore regulations beyond the export ban. Treating cryptographic enablers as dangerous devices similar to explosives, the government could seek to obviate the problems cryptography poses by refusing to allow threatening forms to proliferate domestically.[39] Regulatory options include restrictions on the potency of cryptography available to the public and mandatory key escrow schemes, like the Clinton administration's early Clipper Chip proposal.[40]

---

[35] *Olmstead v United States*, 277 US 438 (1928).

[36] John Markoff, *Secure Digital Transactions Just Got a Little Less Secure*, New York Times A1 (Dec 11, 1995) (cited in note 21).

[37] A "brute-force" attack is what the name implies: using every possible combination of keys to try to crack the code.

[38] See Michael Froomkin, *The Metaphor is the Key: Cryptography, The Clipper Chip and the Constitution*, 143 U Pa L Rev 709, 887 (1995).

[39] By maintaining the export ban on cryptographic software generating keys of greater than 40 bits, the federal government presently seeks to deter the development for domestic use of commercial cryptographic software containing stronger protection. This is because the export ban forces U.S. software manufacturers to produce two versions of software with encrypting capabilities, one of full strength for the domestic market and one for export with much weaker capacities. Export Controls on Mass Market Software, Hearing before the Subcommittee on Economic Policy, Trade and Environment of the House Committee on Foreign Affairs, 103rd Cong, 1st Sess 44-47 (1993) (statement of Ray Ozzie, President of Iris Associates, on behalf of the Business Software Alliance).

[40] Under a mandatory key escrow scheme like the Clipper Chip, the government would only allow individuals to use encrypting technologies which provide the government with a "back door" key which can be entered with a valid search warrant. The implications of the Clipper Chip have already been discussed extensively in legal scholarship. See Froomkin, 143 U Pa L Rev at 752-62 (cited in note 38). See also Comment, *The Fourth Amendment's Prohibitions on Encryption Limitations*, 58 Albany L Rev 467, 502-04 (1995); Ilene Knable Gotts and Alan D. Rutenberg, *Navigating the Global Information Superhigh-*

We must take the "device" analogy seriously because the government itself currently views cryptography as a device as well as a dangerous munition.[41] As such, the government might consider regulation of cryptographic software in the same manner that it considers regulation of other munitions. The Second Amendment is not implicated when the federal government decides to ban certain types of guns or bullets because of their potency; instead, it allows reasonable restrictions on uses which endanger the safety of law-enforcement officials and the general public.[42] The same could occur with cryptography; the government could limit the bit length of keys to restrict them to lengths which the government could decrypt if necessary.[43]

A regulation on the sophistication of cryptographic software seems unlikely to prove effective. Restricting the use of cryptography to more easily decryptable forms defeats the purpose of encrypting data. If the government can decrypt an individual's code, so too could any enterprising private citizens with a background in cryptography. Those users most concerned with the security of their documents, including those who believe they have incriminating information to hide, likely would continue to use encrypting devices with the highest possible security. In addition, cryptographic software does not constitute a "thing" which people can detect and destroy like a forbidden bullet. It is a form of information which users can create, duplicate, and transmit worldwide with greater ease than any tangible asset. The government will have great difficulty stopping the spread of cryptographic software given the ease of international distribution via the Internet.

---

way, 8 Harv J L & Tech 275, 332-36 (1995); Comment, *The Clipper Chip: How Key Escrow Threatens to Undermine the Fourth Amendment*, 25 Seton Hall L Rev 1142, 1165-75 (1995); Lawrence Lessig, *The Path of Cyberlaw*, 104 Yale L J 1743, 1751 n 23 (1995).

[41] 22 CFR § 121.1, Category XIII(b) (1995).

[42] The same argument was used in Congress to ban the use of certain types of bullets which can pierce otherwise "bulletproof" vests. See 18 USC § 922(a)(7)-(8) (1995) (banning the manufacture, import, sale or delivery of "armor piercing ammunition"). In signing the bill, President Reagan noted that " . . . [C]ertain forms of ammunition have no legitimate sporting, recreational, or self-defense use and thus should be prohibited." Ronald Reagan, *Regulation of Armor-Piercing Ammunition*, 22 Weekly Compilation of Presidential Documents 1130 (Aug 28, 1986). See also 18 USC § 929(a)(1) (1995) (increasing the penalty by at least five years for the use of armor piercing ammunition in drug trafficking offenses).

[43] At the same time, licensing and registration of keys could also be mandated, just like with guns. This is the essence of the "Clipper Chip" proposal. See note 40.

B. A Ban On Cryptography Would Violate the First Amendment

1. *Cryptography is a form of speech.*

The government could choose to ban all computer-generated encryption under a "national security" or "needs of law enforcement" justification. Professor Michael Froomkin compares this approach to the "Al Capone" prosecution for tax evasion: if a user will not voluntarily decrypt potentially incriminating evidence for the government, she could still face prosecution for the lesser crime of using illegal cryptography.[44] The First Amendment provides the initial challenge to such a scheme. We should consider whether cryptography is a form of speech. If it is a form of speech, then on what the grounds can the government ban it?

Cryptographic communications (i.e., the documents themselves) should be treated legally as a form of speech. An encrypted document resembles an unknown foreign language in many ways: it consists of alphanumeric characters and exists for no other reason than to express something to others. On the other hand, in its encrypted form it possesses none of the traits we typically associate with speech. The dictionary provides one definition of speech: "the communication or expression of thoughts in spoken words."[45] The receiver of the encrypted communication cannot comprehend it in this form, requiring the use of a mechanical aid for translation. Because it is wholly incomprehensible in that state, some argue that we should not consider it to be speech.[46]

Professor Froomkin, however, reminds us that these Internet communications do not differ from telephonic communications.[47] When one talks on the phone, speech travels through a device which translates it into another form—electric pulses or a fiber-optic signal. The signal itself remains indecipherable to the person at the other end of the line. The courts, however, have consistently seen these communications as forms of expression protected by the First Amendment to the same extent as other oral forms.[48] For example, in *Sable Communications of California, Inc. v FCC*,[49] the Supreme Court struck down certain indecency-

---

[44] Froomkin, 143 U Pa L Rev at 881 n 756 (cited in note 38).

[45] *Webster's Ninth New Collegiate Dictionary* 1133 (Merriam-Webster, 1986).

[46] See Froomkin, 143 U Pa L Rev at 867 (cited in note 38).

[47] Id at 869-70.

[48] See, for example, *Turner Broadcasting System, Inc. v FCC*, 114 S Ct 2445, 2456 (1994) (cable television as speech); *Sable Communications of California, Inc. v FCC*, 492 US 115 (1989) (telephone communications).

[49] 492 US 115 (1989).

based restrictions on telephone communications as overbroad restrictions of free speech. Encrypted documents also exist as a means of communicating thoughts and ideas through a particular medium, and we can safely treat them as speech in examining the legality of encryption.

In the only case to address these issues so far, a district court judge ruled that cryptographic computer source code was speech.[50] Cryptographic source code is the set of instructions which becomes translated into a computer-readable form in order to generate encrypted documents.[51] The *Bernstein* case challenged ITAR restrictions on the export of cryptographic software on their face.[52] In a preliminary order, Judge Patel ruled that source code was speech for First Amendment purposes. "The music inscribed in code on the roll of a player piano is no less protected for being wholly functional. Like source code converted to object code, it 'communicates' to and directs the instrument itself, rather than the musician, to produce the music. That does not mean it is not speech."[53]

1. *Encryption is protected by the First Amendment and cannot be barred under a "national security" or "needs of law enforcement" justification.*

In the interests of law enforcement, the government could issue a total ban on the use of encryption by private citizens. This would not represent the first time that the federal government has attempted such wide-ranging regulation. As part of the Office of Censorship's activities during World War II, the government banned the use of unauthorized codes, ciphers, and secret inks.[54] In addition, Americans could only write letters in English, French, Portuguese, or Spanish; the use of any other lan-

---

[50] *Bernstein v United States Department of State*, 922 F Supp 1426, 1436 (ND Cal 1996).

[51] Id at 1436. While *Bernstein* involved source and object code, its analysis is equally applicable to the question of encrypted documents. Judge Patel explained that a language is "a complex system of understood meanings within specific communities" even when that community is between a person and her computer. As with the encrypted documents themselves, object code carries meaning which is comprehensible only after being processed by a computer. Nevertheless, *Bernstein* finds it to be speech: "[T]he functionality of a language does not make it any less like speech." Id at 1435.

[52] Id at 1428. This opinion represents the denial of a motion to dismiss for lack of justiciability. There has yet to be a ruling on the merits. Id.

[53] Id at 1435.

[54] 32 CFR § 1801.22 (1945).

guage was forbidden.[55] Similar rules permitted only specified languages on certain telephone calls.[56]

It seems highly unlikely that the courts would sustain peacetime restrictions on the languages or modes of communications for telephones and e-mail on First Amendment and equal protection grounds.[57] Professor Geoffrey Stone, in examining the Supreme Court's analysis of the constitutionality of content-neutral laws which sought to ban particular forms of expression,[58] determined that such regulations generally were subject to intermediate scrutiny.[59] In such a test, the Court considers factors such as the substantiality of the government interest, the extent to which the restriction furthers that interest, and the availability of less restrictive alternatives.[60] In order to pass the substantiality test, the government cannot merely demonstrate that less restrictive measures would serve its ends less effectively. Rather, writes Stone, " . . . [t]he government must prove that its use of a less restrictive alternative would seriously undermine substantial government interests."[61] Stone notes that the government often, though not always, loses under this test.[62]

A ban on encryption probably will not survive an intermediate-scrutiny test based on a "needs of law enforcement" justification. In *City of Houston v Hill*,[63] the Supreme Court overturned a local ordinance that criminalized conduct for "willfully or intentionally interrupt[ing] a city policeman . . . by verbal challenge during an investigation."[64] The Court held that the ordinance constituted an overbroad abridgment of free speech by criminalizing a substantial amount of constitutionally protected conduct regardless of whatever legitimate applications the ordinance might have.[65] Because a ban on all cryptography usage would criminalize speech bearing no criminal element whatsoever, the Court likely will not uphold it. This would provide the

---

[55] 32 CFR § 1801.48 (1945). The section also banned the use of "any word, term, phraseology or language having a double meaning."

[56] 32 CFR § 1801.74 (1945).

[57] Froomkin, 143 U Pa L Rev at 865-66 (cited in note 38).

[58] The list included such things as leafletting, door-to-door solicitation, and street demonstrations. Geoffrey Stone, *Content-Neutral Restrictions*, 54 U Chi L Rev 46, 64 (1987).

[59] Id.

[60] Id at 52.

[61] Id at 53.

[62] Stone, 54 U Chi L Rev at 53 (cited in note 58).

[63] 482 US 451 (1987).

[64] Id at 454.

[65] Id at 460-67.

same benefits to law enforcement and investigation as banning doors on private houses and will likely be viewed as unconscionable by the courts.[66]

The Court probably will refuse to uphold such restrictions on the grounds of national security. In *United States v Robel*,[67] the Court struck down a section of the Subversive Activities Control Act of 1950[68] as an unconstitutional abridgment of protected First Amendment activities despite the proferred "national security" justification. The case concerns Cold War restrictions on the employment of Communists at defense facilities. Writing in strong language for the Court, Chief Justice Warren argued: " . . . this concept of 'national defense' cannot be deemed an end in itself, justifying any exercise of legislative power designed to promote such a goal. Implicit in the term 'national defense' is the notion of defending those values and ideals which set this Nation apart."[69] Even national security justifications had to receive protection by the "less drastic" means.[70] As a sweeping ban on all cryptography would have similarly drastic results, such overreaching action appears unlikely to survive such a test.

---

[66] This is not to say, however, that a narrowly tailored statute to increase the penalty for those crimes in which cryptography is used in an effort to hinder investigations might be acceptable. This would be akin to 18 USC § 924(c)(1) (1995), which increases the penalty by five years for the use or carrying of a firearm during and in relation to a crime of violence or drug trafficking, with longer penalties for semiautomatic and other more potent firearms.

[67] 389 US 258 (1967).

[68] 50 USC § 784(a)(1)(D).

[69] *Robel*, 389 US at 264.

[70] Id at 268. Explaining the test, Chief Justice Warren wrote:

> Faced with a clear conflict between a federal statute enacted in the interests of national security and an individual's exercise of his First Amendment rights, we have confined our analysis to whether Congress has adopted a constitutional means in achieving its concededly legitimate legislative goal. In making this determination we have found it necessary to measure the validity of the means adopted by Congress against both the goal it has sought to achieve and the specific prohibitions of the First Amendment. But we have in no way "balanced" those respective interests . . . . Such a course of adjudication was enunciated by Chief Justice Marshall when he declared: "Let the end be legitimate, let it be within the scope of the constitution, and all means which are appropriate, which are plainly adapted to that end, which are not prohibited, but consistent with the letter and spirit of the constitution, are constitutional." *McCulloch v Maryland*, 4 Wheat 316, 421 (1819) (emphasis added). In this case, the means chosen by Congress are contrary to the "letter and spirit" of the First Amendment.

Id at 268 n 20.

C. The Fifth Amendment And Key Escrow

1. *The current state of Fifth Amendment jurisprudence.*

Even if the use of cryptography remains protected, it poses little threat to law enforcement so long as authorities can obtain copies of the "plaintext" desired. The question becomes whether law enforcement agencies could compel users to decrypt their documents and produce plaintext upon the presentation of a valid search warrant or subpoena. Law enforcement officials would not regard cryptography as a threat nor desire a total ban on its use if they could crack the codes when necessary. This capability would give officials access to those documents seized from suspects' hard drives and UNIX accounts. This would not offer a total solution, for it would not eliminate the problem of decrypting documents which authorities obtain surreptitiously by entering user accounts, wiretapping, and enlisting other means to circumvent the owner of the documents. The Fifth Amendment, however, protects individuals from self-incrimination and stands as a substantial bar for the government to clear.

The Self-Incrimination clause reads: "[n]o person . . . shall be compelled in any criminal case to be a witness against himself . . . ."[71] As currently interpreted, the Fifth Amendment prevents an individual from "being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature."[72] At the same time, a criminal suspect can be compelled to produce certain "real or physical evidence."[73]

The privilege against self-incrimination has deep historical roots.[74] In *Holt v United States*,[75] Justice Holmes asserted that the privilege did not bar all attempts to gain evidence from the accused. "The prohibition of compelling a man in a criminal court to be witness against himself is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence when it may be material."[76]

---

[71] US Const, Amend V.

[72] *Schmerber v California*, 384 US 757, 761 (1966).

[73] Id at 764.

[74] For a detailed, informative view of the historical roots of the privilege, see R.H. Helmholz, *Origins of the Privilege Against Self-Incrimination: The Role of the European* Ius Commune, 65 NYU L Rev 962 (1990).

[75] 218 US 245 (1910).

[76] Id at 252-53.

Holmes thus saw no problem in compelling the defendant to wear a blouse in order to prove that it fit his body.[77]

The Supreme Court's decision in *Schmerber v California*[78] established the framework for modern-day self-incrimination analysis. "It is clear that the protection of the privilege reaches an accused's communications, whatever form they might take, and the compulsion of responses which are also communications, for example, compliance with a subpoena to produce one's papers."[79] To receive the protection of the privilege, the act must communicate something substantive about the accused; the Fifth Amendment does not protect "acts noncommunicative in nature as to the person asserting the privilege."[80] The Court reasoned that a compelled blood test did not violate the privilege since the defendant participated simply as a donor and was not required to communicate anything regarding his guilt. Anything incriminating came from the state's chemical analysis of the extracted sample, not from any direct communication by the accused.[81]

Similarly, the Fifth Amendment does not provide an absolute bar to the compelled production of documents by the accused.[82] In *Curcio v United States*,[83] the Court indicated that the government could compel production of corporate documents. Forcing an individual to reveal even the mere location of documents, however, violates the privilege by compelling him to communicate evidence which may be incriminating. "[F]orcing the custodian to testify orally as to the whereabouts of nonproduced records requires him to disclose the contents of his own mind. He might be

---

[77] Id.

[78] 384 US 757.

[79] Id at 763-64 (citing *Boyd v United States*, 116 US 616 (1885)).

[80] Id at 761 n 5. The *Schmerber* court used "testimonial" and "communicative" as synonyms in trying to explain the test:

> But the Fifth Amendment relates only to acts on the part of the person to whom the privilege applies, and we use these words subject to the same limitations. A nod or head-shake is as much a "testimonial" or "communicative" act in this sense as are spoken words. But the terms as we use them do not apply to evidence of acts noncommunicative in nature as to the person asserting the privilege, even though, as here, such acts are compelled to obtain the testimony of others.

Id.

[81] Id at 765.

[82] *United States v Nobles*, 422 US 225 (1975).

[83] 354 US 118 (1957).

compelled to convict himself out of his own mouth. That is contrary to the spirit and letter of the Fifth Amendment."[84]

In *United States v Nobles*,[85] the Court reviewed some of the limits of the privilege's protection. In order to receive protection, the testimony sought from the accused must include incriminating information. The privilege remains personal to the defendant and does not extend to third parties relating incriminating information.[86] Moreover, not all compelled communications incriminate. "The purpose of the relevant part of the Fifth Amendment is to prevent compelled self-incrimination, not to protect private information. Testimony demanded of a witness may be very private indeed, but unless it is incriminating and protected by the Amendment or unless protected by one of the evidentiary privileges, it must be disclosed."[87]

In *Fisher v United States*,[88] the Court explained further how the Fifth Amendment privilege against self-incrimination only provides a limited shield for criminal defendants, leaving unprotected those documents which do not incriminate. "It is also clear that the Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a *testimonial* communication which is incriminating."[89]

Witnesses stand protected, however, from compulsion to "restate, repeat, or affirm the truth of the contents of the documents sought."[90] If the government already knows of the existence and location of the documents and can prove independently their connection to the accused, he does not incriminate himself by producing those documents. Rather, the documents themselves, not the defendant, incriminate. The defendant only has protection from communicating personal guilt. In her concurrence in a subsequent case, Justice O'Connor curtly summarized the prevailing view of the *Fisher* holding: "[T]he Fifth Amendment provides absolutely no protection for the contents of private papers of any kind."[91]

---

[84] Id at 128.

[85] 422 US 225 (1975).

[86] Id at 233.

[87] Id at 233 n 7 (quoting *Maness v Meyers*, 419 US 449, 473-74 (1975) (White concurring in judgment)).

[88] 425 US 391 (1976).

[89] Id at 408.

[90] Id at 409.

[91] *United States v Doe*, 465 US 605, 618 (1984) (O'Connor concurring).

Even when the document itself receives no protection, however, the act of document production can become a form of incriminating testimony protected by the Fifth Amendment.[92] In *United States v Doe*, the Court held that the compelled production of certain business records, under the circumstances, constituted a testimonial act covered by the privilege against self-incrimination. Specifically, the Supreme Court declined to upset the finding of the District Court that "enforcement of the subpoenas would compel [respondent] to admit that the records exist, that they are in his possession, and that they are authentic."[93] The government failed to show that it otherwise could prove the documents' existence, possession, and authenticity with relation to their alleged owner.[94]

In a different case, *Doe v United States*,[95] the question arose concerning the compelled delivery of bank records through a consent decree. During an investigation for suspected fraud and receipt of unreported income, federal investigators subpoenaed Doe's bank records from the Cayman Islands and Bermuda. Only Doe's signature could release the records.[96] Doe argued that signing a consent decree to have the records released would make it a compelled testimonial communication protected by the Fifth Amendment.[97]

Realizing that the release form could become testimonial, the Government drafted the decree to avoid forcing the defendant to admit ownership of the records or vouch for their authenticity.[98] For that reason, the Court held that the decree did not constitute a testimonial communication.[99] The Court reiterated its test that " . . . in order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a 'witness' against himself."[100] Only examining the facts and cir-

---

[92] Id.

[93] Id at 613 n 11 (quoting the lower court's opinion in *In re Grand Jury Empanelled March 19, 1980*, 541 F Supp 1, 3 (1981)).

[94] Id at 613 n 12.

[95] *Doe v United States*, 487 US 201 (1988).

[96] Id at 202-3.

[97] Id at 205-6.

[98] The consent form did not name specific banks; instead, the defendant was to command "any bank or trust company at which I may have a bank account of any kind . . . to disclose all information and deliver copies of all documents of every nature in your possession or control which relate to said bank account . . . ." Id at 204 n 2, 205.

[99] *Doe*, 487 F2d at 219.

[100] Id at 210.

cumstances of the particular case, rather than by the articulation of narrow rules, answers this question.[101]

Justice Stevens, dissenting in the second *Doe* case, adopted an analogy that seems apt to the cryptography debate.[102] Stevens listed the various items which a court could force a defendant to produce, including fingerprints, blood samples, and handwriting specimens. He then stated:

> But can he be compelled to use his mind to assist the prosecution in convicting him of a crime? I think not. He may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe—by word or by deed.[103]

The majority (in dicta) agreed with Stevens's assessment of the distinction but disagreed with his conclusions. According to the majority, where people keep information presents a crucial distinction. "We do not disagree with the dissent that '[t]he expression of the contents of an individual's mind' is testimonial communication for purposes of the Fifth Amendment."[104] This would appear to establish a clear test for Fifth Amendment analysis of encryption codes: does the key to a PGP-encrypted document more closely resemble the key to a strongbox or the combination to a safe?

Most recently, the Court asserted in *Pennsylvania v Muniz*[105] that a de minimus test for whether compelled evidence is testimonial, and thus protected by the privilege, arises when the accused faces what Justice Brennan called the "cruel trilemma."[106] If the only possible responses to a question are "self-accusation, perjury or contempt,"[107] the accused receives the privilege's protection. According to Brennan: "[W]henever a suspect is asked for a response requiring him to communicate an express or implied assertion of fact or belief, the suspect confronts the 'trilemma' of truth, falsity or silence, and hence the

---

[101] Id at 214-15 (citing *Fisher*, 425 US at 410).

[102] Id at 219 (Stevens dissenting).

[103] *Doe*, 487 US at 219 (Stevens dissenting).

[104] Id at 210 n 9.

[105] 496 US 582 (1990).

[106] Id at 597.

[107] Id at 595 n 8 (quoting *Murphy v Waterfront Commission of New York Harbor*, 378 US 52, 55 (1964)).

response (whether based on truth or falsity) contains a testimonial component."[108]

2. *The Fifth Amendment protects users of encryption software from being forced to reveal their private keys.*

The courts likely will find that compelling someone to reveal the steps necessary to decrypt a PGP-encrypted document violates the Fifth Amendment privilege against compulsory self-incrimination. Because most users protect their private keys by memorizing passwords to them and not writing them down, access to encrypted documents would almost definitely require an individual to disclose the contents of his mind.[109] This bars the state from compelling its production. This would force law enforcement officials to grant some form of immunity to the owners of these documents to gain access to them.

Encryption software is designed to protect a user's privacy and privilege against self-incrimination. In order to protect the private key on the hard drive, PGP asks the user to enter a pass phrase of up to 128 characters.[110] An algorithm called MD5 encrypts the pass phrase onto the hard drive.[111] The user must

---

[108] Id at 597.

[109] If the user has written down her password, law enforcement agencies will be able to obtain it via search warrants, subpoenas, and the like.

[110] Users are urged to make the pass phrase as complex as possible, while still being able to commit it to memory:

> All of the security that is available in PGP can be made absolutely useless if you don't choose a good pass phrase to encrypt your secret key ring. Too many people use their birthday, their telephone number, the name of a loved one, or some easy to guess common word. While there are a number of suggestions for generating good pass phrases, the ultimate in security is obtained when the characters of the pass phrase are chosen completely at random. It may be a little harder to remember, but the added security is worth it. As an absolute minimum pass phrase, I would suggest a random combination of at least 8 letters and digits, with 12 being a better choice. With a 12 character pass phrase made up of the lower case letters a-z plus the digits 0-9, you have about 62 bits of key, which is 6 bits better than the 56 bit DES keys. If you wish, you can mix upper and lower case letters in your pass phrase to cut down the number of characters that are required to achieve the same level of security. I don't do this myself because I hate having to manipulate the shift key while entering a pass phrase. A pass phrase which is composed of ordinary words without punctuation or special characters is susceptible to a dictionary attack. Transposing characters or misspelling words makes your pass phrase less vulnerable, but a professional dictionary attack will cater for this sort of thing.

PGP FAQ, § 3.11. How do I choose a pass phrase?, http://www.quadralay.com/www/Crypt/PGP/pgp03.html#311.

[111] Paul Elliot, *EFH Pretty Good Privacy Workshop*,

enter the phrase before each use of PGP, both to encrypt and to decrypt. To further complicate the process, PGP makes its operations unpredictable by the use of human-generated random numbers.[112] This process ensures that a brute-force attempt at discovering the pass phrase can take literally hundreds of millions of years.

Until some other "backdoor" method emerges, decryption of a PGP-encrypted document requires the user to reveal the pass phrase, incriminating herself in the process in violation of the Fifth Amendment. The second *Doe* decision seized on this difference, maintaining that the entire *Schmerber* line of cases barred a suspect from "being compelled to disclose or communicate information or facts that might serve as or lead to incriminating evidence."[113] Being forced to reveal a pass phrase might serve as, or lead to, incriminating evidence.

It also would testify to the user's possession of the encrypted files, for only the actual user would know the correct pass phrase. The instructions for using PGP, as with any form of software privacy protection, urge the user to keep the passwords secret, neither to share them with friends nor to write them down.[114] Therefore, it appears that PGP users remain safe from compulsory revelation of their pass phrases; as such, their documents are probably safe from law enforcement decryption.[115]

---

http://www.efh.org/pgp/pgpwork.html#passphrasesize.

[112] Id. Specifically, PGP asks the user to type for a few seconds. It uses the frequency of the keystrokes to generate the random numbers. So long as the individual does not use the auto-repeat feature on the keyboard, truly random numbers will be produced. An encryption process called IDEA facilitates the conversion. Id.

[113] 487 US at 211 n 10.

[114] Jeff Licquia, *Alt.security.pgp FAQ § 3.12. (How do I remember my pass phrase?)*, http://www.quadralay.com/www/Crypt/PGP/pgp00.html. His answer:

> This can be quite a problem especially if you are like me and have about a dozen different pass phrases that are required in your everyday life. Writing them down someplace so that you can remember them would defeat the whole purpose of pass phrases in the first place. There is really no good way around this. Either remember it, or write it down someplace and risk having it compromised.

Id.

[115] There is still the prospect of governmentally granted immunity in certain cases if it deems the information vital enough. In national security cases, for example, the contents of the information may be the most vital interest for the government. See Phillip Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U Chi Legal F 171.

CONCLUSION

If the government seeks to force a solution to the problem cryptography poses to law enforcement, it will violate the First and Fifth Amendments as currently understood. All potential gains to law enforcement are offset by the destruction of true privacy and individual rights in cyberspace. FBI Director Louis Freeh has testified that encryption is posing an increasing roadblock for investigations of espionage cases, child pornographers, drug traffickers, and militia groups.[116]

The issue rests on trust: if one fears narcoterrorists and espionage agents, not to mention mundane criminals like the Mafia, then some means of assisting law enforcement officials in their tasks needs to exist. Were this an issue of policy, fertile grounds for debate would exist here. One could engage in all sorts of balancing tests to determine whether the interests of cryptography users outweighed those of the state. However few and rare, cases exist in which most of us would believe that the government should have access to encrypted documents. For example, if the government believes that the export of sensitive nuclear secrets to enemies of the state breaches national security, then it should have the ability to intervene.

But if the government knows that people are distributing classified documents, then it already has sufficient information to intervene. Because encrypted documents do not disclose their own contents, government suspicion about a communication means that it already possesses extrinsic incriminating evidence.[117] Indeed, these crimes cannot take place solely in the encrypted world: real-life actions such as theft or distribution of illegal goods must occur as well for harm to arise. These tangible harms can still be prosecuted.

Cryptography does alter the equation for law enforcement, but these new dangers cannot force an overturning of our rights

---

[116] Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1996, Hearings on S 1726 before the Senate Committee on Commerce, Science, and Transportation, 104th Cong, 2d Sess (July 25, 1996) (testimony of Louis J. Freeh, Director, Federal Bureau of Investigation).

[117] According to William R. Spernow, a computer crime specialist who has worked with the Federal Bureau of Justice Assistance on several encryption-related cases, including one in which a pedophile encrypted the identities of his young victims, "'In cases where there's encryption, the officers have been able to make the case through other investigative means. . . . If we hustle, we can still make our cases through other kinds of police work.'" Steven Levy, *The Cypherpunks vs. Uncle Sam*, New York Times Magazine 46, 49 (June 12, 1994) (cited in note 18).

under the Constitution. Justice Brandeis' dissent in *Olmstead v United States* is as true today as it was in 1928: "Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding."[118]

[118] 277 US 438, 479 (1928) (Brandeis dissenting).