



Privacy in the Digital Age: Encryption Policy—A Call for Congressional Action

DAVID B. WALKER*

CITE AS: 1999 STAN. TECH. L. REV. 3

http://stlr.stanford.edu/STLR/Articles/99_STLR_3

I. INTRODUCTION

¶ 1 With the advance of the Internet and the development of sophisticated digital communication tools, individuals and corporations have pressed for continual advances in encryption and other privacy and security enhancing measures. The broad dissemination of strong encryption is seen by many as a critical precursor to effectively tapping the commercial potential of the Internet. As the technology has advanced, the concerns of law enforcement have also become more acute. Alarmed that strong encryption will bar law enforcement and national security agencies from monitoring the illicit communications of criminals and foreign nationals opposing U.S. interests, the government has restricted the export of strong encryption and has proposed various means to provide “back-door” access to data by law enforcement under certain circumstances, including key escrow.

¶ 2 This paper will analyze the trends in the law surrounding digital on-line privacy today and anticipate the implications for the future. It will be argued that the courts have historically had difficulty applying the Fourth and Fifth Amend-

* J.D., 1999, Stanford Law School; M.S.A.A., 1990, Stanford University. Law clerk (1999-2001 term) to the Hon. Haldane Robert Mayer, Chief Judge, U.S. Court of Appeals for the Federal Circuit. The author would like to thank Professors Kathleen M. Sullivan and George Fisher of Stanford Law School for their helpful critiques of this manuscript.

ments to new and emerging technologies to protect the challenges to individual privacy posed by new technologies and, as a result, have tended to under-protect those privacy interests. Historical instances of congressional intervention to raise the privacy standard by limiting law enforcement access to telephone and electronic communications under Title III and the Electronic Communications Privacy Act, respectively, will be addressed. In addition, the development of strong encryption and federal attempts to regulate its use will be evaluated in their historical context. The concerns of the federal government will be analyzed, as will the extent to which the technological advances involving strong encryption represent a quantum leap that creates a compelling government interest in the ability to bypass privacy measures taken by individuals and corporations. The government's proposed key escrow plan will be evaluated as to whether it represents a search under the Fourth Amendment and whether the requirement to escrow the encryption key implicates the Fifth Amendment. It will be argued that the threshold tests present in the current legal precedent create an opportunity to structure a key escrow program that will fall outside the ambit of the Fourth and Fifth Amendments and thus be Constitutionally permissible. The merits of mandatory key escrow will be discussed and it will be argued that the significant sacrifice of personal privacy and the commercial disadvantage to the U.S. encryption industry caused by the current export control regime and the proposed key escrow programs far outweigh the limited benefit to law enforcement and national security interests that would actually be realized by implementing a mandatory national key escrow program. The risk of such "under-protection" of individual privacy interests is sufficiently great as to necessitate congressional action to once again restore the balance between law enforcement and national security and individual privacy and to prevent the considerable harm being done by the current and proposed Clinton Administration policies regarding encryption. By mapping out the state of the law and the historical antecedents of the current government attempts to control the implementation of new technologies, this paper will seek to frame the nature of privacy and the proper balance between government interests in national security and prosecuting criminals and the individual desire to be left alone. It will be argued that Congress can restore that balance by implementing legislation similar to the SAFE bill, which prohibits mandatory key escrow and permits the export of encryption software that is freely available in the world market.

II. HISTORY OF CONGRESSIONAL ACTION

¶ 3 The courts have historically had difficulty applying the strictures of the Fourth and Fifth amendments to new and emerging technology and have had a tendency to apply existing legal tests created at a time when the new technology was inconceivable. On prior occasions, the result has sometimes been to under-protect individual privacy interests, necessitating congressional action to provide adequate protection. To put the respective roles of the judiciary and Congress in perspective, it is useful to consider the historical development of the law governing electronic surveillance and the efforts of the courts to grapple with the challenges posed by technological advances in eavesdropping technology and the spread of the use of computers for interpersonal communications.

A. Title III

¶ 4 Concern with electronic surveillance tools and their use to invade the private conversations of individuals is not new.¹ Electronic surveillance encompasses a broad array of technologies that allow the user to monitor and record private conversations, to monitor the movements of persons and objects, and to trace or record calls made to or from a particular telephone. Law enforcement has historically found electronic surveillance to be an invaluable tool to monitor criminal activity and to gather evidence for later use in criminal prosecutions. These same law enforcement officials have found themselves before the courts when those efforts were claimed to violate the constitutional rights of those being monitored.² The Supreme Court gave its most detailed pronouncement to date regarding electronic surveillance in *Berger v. New York*.³ At issue in *Berger* was a New York eavesdropping statute in which the sole requirement for an order to issue was that a state law enforcement agent avow that there was reasonable ground to believe that evidence of a crime could thus be obtained.⁴ The Supreme Court found this standard deficient on its face and set forth six grounds on which it fell short of

¹ The Supreme Court addressed the use of electronic surveillance by law enforcement agencies as early as the 1920s. See *Olmstead v. United States*, 277 U.S. 438 (1928) (upholding a warrantless wiretap from outside the defendant's premises since no trespass was committed).

² See *Katz v. United States*, 389 U.S. 347 (1967) (excluding conversations obtained by attaching a listening device to a phone booth without a warrant as "violat[ing] the privacy upon which [the defendant] justifiably relied while using the telephone booth" and implicating the Fourth Amendment).

³ 388 U.S. 41 (1967).

⁴ See *id.* at 54.

Fourth Amendment warrant requirements.⁵ Recognizing the potential for abuse through the unfettered use of electronic surveillance and following the lead of the Supreme Court, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968⁶ (hereinafter “Title III”) which preempted state eavesdropping laws⁷ and imposed procedural safeguards to individual privacy even more stringent than those mandated by the courts. As originally enacted, Title III pertained only to wire and oral communications.⁸

¶ 5

Title III created stringent procedural requirements to obtain authorization to conduct electronic surveillance, including the requirement to obtain a court order prior to intercepting the communications and permitting their intercept only for certain enumerated crimes.⁹ Additionally, only state and federal law enforcement officers and attorneys authorized to investigate or prosecute offenses enumerated under 18 U.S.C. § 2516 may apply for such a court order,¹⁰ and the application

⁵ The New York statute was considered deficient because: (1) it did not require a showing of probable cause that a particular offense had been or was being committed; (2) it failed to require a particularized showing of what conversations would be seized; (3) it allowed a two-month monitoring period on a single showing whereby all conversations, not just incriminating ones, could be seized; (4) it provided for no termination date once the target conversations were obtained; (5) it lacked the notice requirement of conventional warrants and permitted uncontested entry without any showing of exigency; and (6) it did not require return on the warrant, complicating judicial supervision. *See id.* at 58-60.

⁶ 18 U.S.C. §§ 2510-2520 (1970). *See* S. REP. NO. 1097, at 66 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2177, 2187 (discussing constitutional standards established in *Berger* and *Katz* and the legislative history of Title III).

⁷ A state court judge may grant an eavesdropping order only if the entire process conforms to Title III. 18 U.S.C. § 2516(2). It is clear, however, that Congress intended for states to be able to enact more stringent requirements to authorize electronic surveillance. S. REP. NO. 1097.

⁸ Wire communication is defined as

any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication.

18 U.S.C. § 2510(1).

Oral communications are defined as “any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation.” 18 U.S.C. § 2510. The legislative history of Title III suggests that the language defining oral communications would not cover conversations in certain quasi-public areas such as jail cells or open fields. *See* S. REP. NO. 1097 at 89-90.

⁹ *See* 18 U.S.C. § 2516.

¹⁰ An application must include a full and complete statement of the alleged offense, the facilities where the communications are to be intercepted, a particular description of the communications to be intercepted, the identity of the persons committing the offense, if known, and of whose communications are to be intercepted, a full and complete statement of what other investigative procedures have tried and failed or why they appear unlikely to succeed or too dangerous, and a full and complete statement of the period of time for which the interception is to be maintained. *See* 18 U.S.C. § 2518(1).

must be authorized by the United States Attorney General or a specially designated Assistant or Deputy Attorney General in the Criminal Division.¹¹ A defendant can challenge the government's affidavit on a substantial preliminary showing that a false statement was included in the warrant affidavit knowingly and intentionally or with reckless regard for the truth.¹² If the false statement is necessary to a showing of probable cause, any evidence seized pursuant to that warrant must be suppressed.¹³ A court may issue a surveillance order for the interception of wire or oral communications only if it finds probable cause to believe that (1) a person is committing one of the crimes enumerated in Title III, (2) communications concerning such an offense will be obtained through interception, and (3) the facilities from which the communications are to be intercepted are being used in connection with the commission of the offense.¹⁴ The order, once issued, will specify the location of the intercept, the person whose communications are to be intercepted, if known, the type of communications to be intercepted and the crime to which they pertain, and the authorized duration of the interception.¹⁵ The surveillance must "terminate upon attainment of the authorized objective" and the authorized period must not exceed thirty days, without an extension.¹⁶

¶ 6

Once the intercept has been authorized the law enforcement agents have a duty to minimize any unauthorized interception of communications.¹⁷ If intercepted conversations implicate crimes not covered by the original order, the government must request a determination by the court that the intercept complied with Title III prior to using the evidence.¹⁸ Further safeguards to protect confidentiality require the court to seal the application for intercept authority, the court order granting authority, and all recordings made pursuant to it immedi-

¹¹ See 18 U.S.C. § 2516.

¹² See 18 U.S.C. § 2518(1)(e).

¹³ See *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978).

¹⁴ See 18 U.S.C. § 2518(3). The court must also specifically find that other investigative techniques have failed, appear unlikely to succeed, or would be too dangerous. *Id.*

¹⁵ See 18 U.S.C. § 2518(4).

¹⁶ 18 U.S.C. § 2518(5).

¹⁷ See 18 U.S.C. § 2518(5). See also *Scott v. United States*, 436 U.S. 128, 136-37, 141-43 (1978) (minimization effort must be reasonable in light of objective assessment of officer's actions rather than officer's subjective intent because language of statute focuses on officer's conduct rather than motive; not per se unreasonable that only 40% of intercepted calls clearly related to crimes cited in court order; interception of other conversations reasonable given brief duration or ambiguous nature of contents).

¹⁸ See 18 U.S.C. § 2517(5) (1970).

tely upon completion of the authorized surveillance period.¹⁹ Once the surveillance is complete, an inventory, including notice of the authorization order or application, the surveillance dates, and whether any interception occurred, must be served on the persons named in the surveillance order and, as the judge may require, other persons whose conversations have been intercepted.²⁰ Aggrieved persons may move for suppression if their oral or wire communication were unlawfully intercepted,²¹ if the order authorizing the surveillance was technically insufficient²² or insufficient on its face,²³ or if the interception violated the grounds of the order.²⁴ The statutory exclusionary rules apply in both federal and state proceedings.²⁵ As early as 1968, when Title III was enacted, Congress felt it necessary to create an elaborate framework to monitor and restrict the surveillance of private conversations by the government, over and above the Supreme Court's interpretation of the Fourth Amendment in *Katz* and *Berger*.

B. *Electronic Communications Privacy Act*

¶ 7

As communications technology advanced beyond the congressional definition of wire and oral communication in the 1970s and 1980s, there once again developed a mismatch between the state of the law and the state of technology. Once again, rather than leaving the application of the existing doctrine to the new technologies to the courts, Congress enacted significant reforms to Title III, known as the Electronic Communications Privacy Act of 1986²⁶ (hereinafter "ECPA"). The ECPA added a new form of protected communications, electronic communication,²⁷ that would be treated in a qualitatively different fashion than

¹⁹ See 18 U.S.C. § 2518(8)(a). Failure to properly seal the communications will result in exclusion of the evidence. See *id.* The exclusionary remedy of this section applies not only failure to seal, but also to delay in sealing. See *United States v. Ojeda Rios*, 495 U.S. 257, 264 (1990).

²⁰ See 18 U.S.C. § 2518(8)(d).

²¹ See 18 U.S.C. § 2518(10)(a)(i).

²² See *United States v. Donovan*, 429 U.S. 413, 437 (1977) (quoting *United States v. Chavez*, 416 U.S. 562, 578 (1974)) (holding that suppression is required only for failure to satisfy those Title III provisions that play a "central, or even functional, role in guarding against unwarranted use of wiretapping or electronic surveillance").

²³ See 18 U.S.C. § 2518(10)(a)(ii).

²⁴ See 18 U.S.C. § 2518(10)(a)(iii).

²⁵ See 18 U.S.C. §§ 2515, 2518(a) (1970).

²⁶ Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.

²⁷ "[E]lectronic communication" means

wire and oral communications. According to the legislative history of the ECPA, “a communication is an electronic communication protected by federal wiretap law if it is not carried by sound waves and cannot be fairly characterized as containing the human voice.”²⁸ This definition extends to electronic mail, computer-to-computer communications, microwave transmissions, cellular telephones, and satellite communications.

¶ 8

While the differences among the definitions of various forms of communications covered by Title III as amended by the ECPA may seem semantic, the classification of a particular communication as one form or another can be highly determinative of the outcome in certain situations. Any government attorney can authorize an application for an electronic communication interception, unlike wire or oral communications.²⁹ Perhaps most notably, the statutory exclusionary rules expressed in 18 U.S.C. §§ 2515, 2518(a) do not apply to the interception of electronic communications.³⁰ The ECPA also recognizes the reality that electronic communications are frequently stored either on individual computers or archived on networks, making it possible for law enforcement to access stored electronic communications once they have reached their intended destination or been stored at some network waypoint as well as intercepting them in transit.³¹ The substantive and procedural requirements for authorization to intercept electronic communications are considerably more stringent than those for accessing stored electronic communications.³² The critical distinction between

any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) any wire or oral communication.

(B) any communication made through a tone-only paging device.

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

18 U.S.C. § 2510(12) (1988).

²⁸ S. REP. NO. 541, at 23 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3355, 3563-64.

²⁹ *See* 18 U.S.C. § 2516(3) (1988).

³⁰ *See* 18 U.S.C. § 2510(c); *see* S. REP. NO. 541, *reprinted in* 1986 U.S.C.C.A.N. at 3577 (provision has no effect on constitutional violations under Fourth Amendment involving the interception of electronic communications). *But see* 18 U.S.C. § 2511 (1988) (providing criminal penalties for intentional interception, disclosure, or use of wire, oral, or electronic communications); 18 U.S.C. § 2520 (1988) (authorizing recovery of civil damages for interception, disclosure or intentional use of wire, oral, or electronic communications); 18 U.S.C. § 2701 (1988) (providing criminal penalties for unauthorized access of stored electronic communications or exceeding access authority to such communications).

³¹ The ECPA added statutory provisions explicitly restricting access to stored electronic communications. *See* 18 U.S.C. §§ 2701-11 (1988).

³² *Steve Jackson Games v. United States Secret Service*, 36 F.3d 457, 463 (5th Cir. 1994).

“intercepting” electronic communications during the transmission phase and “accessing” electronic communications during the storage phase governs the applicable section of the ECPA and, subsequently, the requirements for obtaining a warrant to intercept or access the communications.³³ “During the transmission phase, any protection against unlawful interception under Title III is governed by §2511.”³⁴ This necessitates the more elaborate § 2518 warrant (hereinafter “Title III warrant”).

¶ 9

The courts that have reviewed this issue have taken a narrow view of what constitutes transmission of electronic communications. In *Steve Jackson Games v. United States Secret Service*, the Fifth Circuit held that the seizure of a computer used to operate an electronic bulletin board system and containing private electronic mail that had been sent to the bulletin board but not read by the intended recipients was not an unlawful intercept under the Federal Wiretap Act.³⁵ The reasoning for that conclusion was that e-mail cannot be “intercepted” in violation of § 2511(1)(a) when the acquisition of the contents was not contemporaneous with the transmission of those communications.³⁶ In short, even if the e-mail has not reached its final destination, it can only be intercepted if it is actually in transit at the moment of interception.³⁷ The inclusion of the word “transfer” in the definition of “electronic communication,” and omission of the word “transfer” from the phrase “any electronic storage of such communication” in the definition of “wire

Obviously, when intercepting electronic communications, law enforcement officers cannot know in advance which, if any, of the intercepted communications will be relevant to the crime under investigation, and often will have to obtain access to the contents of the communications in order to make such a determination. Interception thus poses a significant risk that officers will obtain access to communications which have no relevance to the investigation they are conducting. That risk is present to a lesser degree, and can be controlled more easily, in the context of stored electronic communications, because, as the Secret Service advised the district court, technology exists by which relevant communications can be located without the necessity of reviewing the entire contents of all of the stored communications. For example, the Secret Service claimed (although the district court found otherwise) that it reviewed the private E-mail on the BBS by use of key word searches.

Id.

³³ See *United States v. Moriarty*, 962 F. Supp. 217, 220 (D. Mass. 1997). *But see* *United States v. Smith*, 155 F.3d 1051, 1057-58 (9th Cir. 1998) (rejecting a narrow interpretation of the term “intercept” with respect to stored wire communications).

³⁴ *Moriarty*, 962 F. Supp. at 220.

³⁵ See 36 F.3d at 460-64.

³⁶ See *id.* See also *United States v. Turk*, 526 F.2d 654, 658 (5th Cir. 1976) (replaying previously recorded conversation is not an intercept because an “intercept” as defined prior to the ECPA, “require[s] participation by the one charged with an ‘interception’ in the contemporaneous acquisition of the communication through the use of the device”).

³⁷ “On arrival in storage, the same messages are subject to §2701.” *Moriarty*, 962 F. Supp. at 220.

communication” reflect that Congress did not intend for “intercept” to apply to “electronic communications” when those communications are in “electronic storage.”³⁸

¶ 10 “Generally, a search warrant, rather than a court order, is required to obtain access to the contents of a stored electronic communication.”³⁹ In *Davis v. Gracey*, the Tenth Circuit held that the incidental seizure of e-mail under a valid warrant to seize computer equipment was not a Fourth Amendment violation.⁴⁰ The court also made clear its position that this incidental seizure did not authorize the subsequent search or retention of the stored files without a warrant,⁴¹ and that a § 2703 warrant rather than a § 2518 court order would have provided the appropriate authorization.⁴² “[O]ther requirements applicable to the interception of electronic communications, such as those governing minimization, duration, and the types of crimes that may be investigated, are not imposed when the communications at issue are not in the process of being transmitted at the moment of seizure, but instead are in electronic storage.”⁴³

¶ 11 Of particular impact to the “private doorbell” program that will be discussed in Part III.D., *infra*, is the fact that providers of electronic communication services are given explicit authority to monitor electronic communications.⁴⁴ The Ninth Circuit has considered an airline, through its computerized travel reservation

³⁸ *Steve Jackson Games*, 36 F.3d at 461-462. See also *Smith*, 155 F.3d at 1057 (“Consequently, in cases concerning ‘electronic communication[s]’—the definition of which specifically includes ‘transfer[s]’ and specifically excludes ‘storage’—the ‘narrow’ definition of ‘intercept’ fits like a glove; it is natural to except non-contemporaneous retrievals from the scope of the Wiretap Act.”); *Wesley College v. Pitts*, 974 F. Supp. 375, 387 (D. Del. 1997) (concluding that Congress did not intend to include the acquisition of electronic communications in electronic storage within the definition of “intercept.”).

³⁹ *Steve Jackson Games*, 36 F.3d at 462 n.7 (referring to 18 U.S.C. § 2703). Message held in storage less than 180 days may only be accessed with a search warrant, while messages held in storage for greater than 180 days may be obtained either via a search warrant or pursuant to an administrative subpoena, grand jury subpoena, or a court order after giving notice to the customer or subscriber to the electronic communications service. 18 U.S.C. § 2703 (1988).

⁴⁰ 111 F.3d 1472 (10th Cir. 1997).

⁴¹ See *id.* at 1480.

⁴² See *id.* at 1483.

⁴³ *Steve Jackson Games*, 36 F.3d at 463.

⁴⁴ See 18 U.S.C. §§ 2511(2)(a)(i), 2701(c)(1) (1988). § 2511(2)(a)(i) states:

It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of service or to the protection of the rights or property of the provider.

18 U.S.C. § 2511(2)(a)(i).

system, to be “a provider of wire or electronic communication service” and its employee to be acting within the scope of her employment by monitoring apparent misuse of the airline’s electronic communication service in accordance with the ECPA.⁴⁵ In *United States v. McLaren*, the court set forth a three-step analysis for determining if a provider acted in accordance with the ECPA in monitoring cellular phone calls.⁴⁶ The court required “some substantial nexus between the use of the telephone instrument to be monitored and the specific fraudulent activity being investigated.”⁴⁷ This does not, however, compel compliance “with the requirement of ‘minimization’ and the other strictures imposed upon judicially authorized Title III wire taps under § 2518(5) because there is simply nothing in the statute that says so, and there is nothing suggesting that Congress intended it.”⁴⁸ It is worthy of note that even these limited restrictions are only applicable to contemporaneous intercept and not to access while in electronic storage. Considering the narrow interpretation of “intercept,” this should not affect efforts to access stored e-mail or voice mail even if they have not been read or played back by their intended recipients. The ECPA provides even more sweeping authority by stating that § 2701(a), which outlines the offense of unlawful access to stored communications, “does not apply with respect to conduct authorized by the person or entity providing a wire or electronic communications service.”⁴⁹

¶ 12

Intercept is very narrowly construed by *Steve Jackson Games* to be contemporaneous with transmission, effectively giving providers of electronic communication services, which include everyone from airlines to Internet Service Providers (ISPs), virtually unfettered access to their users’ and employees’ stored e-mail and voice mail. Corporate providers of electronic communication services

⁴⁵ See *United States v. Mullins*, 992 F.2d 1472 (9th Cir. 1993).

⁴⁶ 957 F. Supp. 215 (M.D. Fla. 1997).

First, the court [sic] must consider whether the provider of electronic communication service had reasonable cause to suspect that its property rights were being abused by a particular subscriber before it began to monitor that subscriber’s phone. Second, the Court must consider whether the interception activities were conducted upon . . . a “permissible” cellular phone. Third, the Court must consider whether the interception activities were reasonable.

Id. at 218.

⁴⁷ *Id.* at 219.

⁴⁸ *Id.* at 220.

⁴⁹ 18 U.S.C. § 2701(c)(1). See *Bohach v. City of Reno*, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (“§ 2701(c)(1) allows service providers to do as they wish when it comes to accessing communications in electronic storage”). In *Bohach*, the City was the “provider” and the Court found that, as a result, neither the City nor its employees could be held liable under § 2701. *Id.*

such as e-mail and voice mail may freely monitor the stored e-mail and voice mail of their employees under *Bohach v. City of Reno*, and can actively intercept such transmissions with reasonable cause and a substantial nexus between the monitored use and the fraudulent activity as long as the monitoring is conducted in a reasonable manner under *McLaren*. If law enforcement agencies wish to gain access to e-mail or voice mail, an ECPA warrant under § 2703 is the appropriate authority and is not bound by minimization and other strictures of the Title III (§ 2518) court order under *Steve Jackson Games*. It should be possible in most cases for law enforcement agents to obtain as much information as required through access of stored electronic messages without ever entering the narrow window of an electronic communication intercept under § 2511, considering that most electronic communications are archived either at the point of origin, the point of receipt, or on the network at some waypoint along the transit path. Though not as stringent as Title III, the ECPA represents a significant effort by Congress to provide additional protection for the privacy of electronic communications beyond that provided by the judicial interpretation of the Fourth Amendment. Recognizing that technological developments had outstripped the capability of prior legislation, namely Title III, to protect reasonable expectations of privacy in personal communications from unwarranted government intrusion, Congress repeated its prior pattern of “raising the bar” to protect the privacy interest of individual Americans.

III. ENCRYPTION

¶ 13 Technology has not, however, stagnated since 1986 but rather has grown at a rate that few anticipated. The development and availability of strong encryption capable of rendering private electronic communications and transactions unreadable to any but the intended recipients has proceeded alongside rapid advances in computing speed and the capability to “break the codes” believed unbreakable a scant few years ago. Interests in the privacy and security of both personal messages and the growing number of electronic commerce transactions compete with governmental interests in prompt access to the plaintext of messages encrypted by criminals and terrorists. To provide a framework for the discussion to follow, some of the fundamentals of encryption technology will first be addressed and then the regulation of encryption by the Clinton Administration and the congressional and industry responses to that regulation will be considered.

A. *Encryption Theory*

¶ 14 Encryption is the transformation of data into an unreadable form. Its purpose is to ensure privacy by keeping information hidden from anyone for whom it is not intended, even those who have access to the encrypted data. Electronic keys are long binary numbers, ones and zeros numbering forty digits or longer, which are used by encryption software⁵⁰ to convert data prior to transmitting it or delivering it to the intended recipient. The intended recipient then uses a key to decrypt the data into readable form. In some encryption systems, known as symmetric-key systems, the same key is used to encrypt as to decrypt the data. In others, such as public-key encryption systems, different keys are used to encrypt and to decrypt the data. Encryption may also be used to authenticate the sender through the use of a digital signature and to verify the time of “signing” a message by attaching a secure digital timestamp.⁵¹ Encryption is becoming a central fixture in the burgeoning electronic commerce industry.

1. *Symmetric-key Encryption*

¶ 15 Symmetric-key is the more traditional form of cryptography, in which a single key can be used to encrypt and decrypt a message. Due to our unfamiliarity with binary numbers, people usually deal with passwords or pass phrases rather than with the encryption keys directly.⁵² The use of a single key intro-

⁵⁰ See Jim Heath, Down to details: how electronic encryption works (visited Nov. 30, 1998) < <http://www.viacorp.com/crypto.html> > .

Encryption software isn't like ordinary software: if there's a small flaw in ordinary software, it may only mean that in certain cases a spell checker doesn't catch a mistake, or the keyboard locks up in some rare circumstances. With encryption software, a small flaw can let experts—benign or malicious—walk right in. And the intrusion probably won't be noticed until a lot of damage is done.

Id.

⁵¹ See RSA Laboratories, FAQ 4.0: Frequently Asked Questions About Today's Cryptography: What is Cryptography? (visited Nov. 29, 1998) < <http://www.rsa.com/rsalabs/faq/html/1.2.html> > .

⁵² See Heath, *supra* note 50. If they know what they're doing, they may pick something like:

ruBRbeQ5mod,**&_ocOEan99[

The encryption software turns that into a binary number. Then uses that number (key) to encrypt all outgoing messages. The mathematical module used for encrypting the message is called the algorithm. The whole system is referred to as a cipher.

At the receiving end, each incoming message is decrypted using the same key. The receiver types in the agreed pass phrase, the software converts it to the binary key, and uses that to decrypt the ciphertext (the incoming encrypted message). Out of that comes plaintext—the original message, in readable form.
Id.

duces the significant but not insurmountable problem of getting the sender and receiver to agree on the secret key without anyone else finding out.⁵³ This requires a method, commonly known as a key agreement protocol, by which the two parties can communicate without fear of eavesdropping.⁵⁴ Some methods of key agreement protocol include the Diffie-Hellman key agreement protocol⁵⁵ and digital envelopes.⁵⁶ A variety of ciphers, or encryption systems, have been developed and are currently in use for symmetric-key cryptography.

¶ 16

DES, an acronym for the Data Encryption Standard, is the best known and most widely used symmetric algorithm in the world, and thus has been extensively studied since its publication.⁵⁷ The DES has a 64-bit block size and uses a 56-bit key during execution via a 16-round Feistel cipher; it was originally designed for implementation in hardware.⁵⁸ Since a 56-bit key is used, there are 2⁵⁶

⁵³ See RSA Laboratories, FAQ 4.0: Frequently Asked Questions About Today's Cryptography: What is Secret-key Cryptography? (visited Nov. 29, 1998) < <http://www.rsa.com/rsalabs/faq/html/2-1-2.html> > .

⁵⁴ See RSA Laboratories, FAQ 4.0: Frequently Asked Questions About Today's Cryptography: What is a Key Agreement Protocol? (visited Nov. 29, 1998) < <http://www.rsa.com/rsalabs/faq/html/2-2-3.html> > (Key agreement protocols allow people to share keys freely and securely over any insecure medium, without the need for a previously established shared secret).

⁵⁵ The Diffie-Hellman key agreement protocol involves the exchange of randomly generated private values that have been mathematically manipulated to generate public values. When each participant mathematically combines his private value with the public value received from the other participant, the result is a common key known only to the two participants. See RSA Laboratories, FAQ 4.0: Frequently Asked Questions About Today's Cryptography: What is Diffie-Hellman? (visited Nov. 29, 1998) < <http://www.rsa.com/rsalabs/faq/html/3-6-1.html> > .

⁵⁶ The digital envelope consists of a message encrypted using symmetric-key cryptography and a symmetric key, usually encrypted with public-key cryptography, but not necessarily. If the participants have an established secret key, they could use this to encrypt the symmetric key in the digital envelope. See RSA Laboratories, FAQ 4.0: Frequently Asked Questions About Today's Cryptography: What is a Digital Envelope? (visited Nov. 29, 1998) < <http://www.rsa.com/rsalabs/faq/html/2-2-4.html> > . In the case where public-key cryptography is used to encrypt the symmetric key, the sender would use the recipient's public key to encrypt the symmetric key and then encrypt the message using the symmetric key prior to sending the encrypted message and key to the recipient. The recipient then uses his private key to decrypt the symmetric key and uses that symmetric key to decrypt the message into readable form. It is possible to send the message to multiple recipients using a single symmetric key by attaching multiple copies of the symmetric key encrypted with each individual recipient's private key. *Id.*

⁵⁷ See RSA Laboratories, FAQ 4.0: Frequently Asked Questions About Today's Cryptography: What is DES? (visited Nov. 29, 1998) < <http://www.rsa.com/rsalabs/faq/html/3-2-1.html> > .

⁵⁸ See *id.*

A block cipher [like the Feistel cipher] is a type of symmetric-key encryption algorithm that transforms a fixed-length block of plaintext (unencrypted text) data into a block of ciphertext (encrypted text) data of the same length. This transformation takes place under the action of a user-provided symmetric key. Decryption is performed by applying the reverse transformation to the ciphertext block using the same symmetric key. The fixed length is called the block size, and for many block ciphers, the block size is 64 bits. In the coming years the block size will increase to 128 bits as processors become more sophisticated.

or 7.2×10^{16} possible key combinations available. No easy attack on DES has been discovered, despite the efforts of researchers over many years. The obvious method of attack is a brute-force exhaustive search of the key space; this process takes 2^{55} steps on average and is therefore highly computationally intensive.⁵⁹ Nevertheless, since IBM first published DES in 1975, computing power has increased by orders of magnitude to the point where DES is no longer considered secure.⁶⁰ The impending demise of DES has been reinforced by a series of “DES-cracking” contests sponsored by RSA Data Security, a prominent producer of encryption products. The rapid advance of encryption-breaking technology has been graphically shown by the drastic reduction in the time required to break the DES algorithm from the first contest in January 1997, which required 96 days, to the most recent contest, held in January 1999, when the algorithm was broken and the secret message converted to plaintext in less than 23 hours using “commonly available technology.”⁶¹ As a follow-on to the DES cipher, the U.S. Government intends to use a triple-DES algorithm, which requires the use of three DES keys, until the Advanced Encryption Standard (AES) is ready for general use.⁶² The security of symmetric-key cryptography is enhanced by frequently changing symmetric keys to prevent their compromise through cryptanalysis or other means.⁶³

RSA Laboratories, FAQ 4.0: Frequently Asked Questions About Today's Cryptography: What is a Block Cipher? (visited Nov. 29, 1998) < <http://www.rsa.com/rsalabs/faq/html/2-1-4.html> > .

⁵⁹ See RSA Laboratories, FAQ 4.0: Frequently Asked Questions About Today's Cryptography: Has DES Been Broken? (visited Nov. 29, 1998) < <http://www.rsa.com/rsalabs/faq/html/3-2-2.html> > .

⁶⁰ The consensus of the cryptographic community is that DES, if not currently insecure, will soon be insecure, simply because 56 bit keys are becoming vulnerable to exhaustive search. As of November 1998, DES was no longer allowed for U.S. government use. See *id.*

⁶¹ See RSA Code-Breaking Contest Again Won by Distributed.Net and Electronic Frontier Foundation (EFF), PR NEWSWIRE, Jan. 19, 1999. This reduced the prior time by more than a factor of two since the “EFF DES Cracker,” which was built for less than \$250,000, had determined the symmetric DES key in 56 hours in July 1998. See Jacqueline Emigh, *DES Code Cracked In 2 Days, 8 Hours*, NEWSBYTES NEWS NETWORK, July 17, 1998, available in 1998 WL 11724349.

⁶² On January 2, 1997 the AES initiative was announced and on September 12, 1997 the public was invited to propose suitable block ciphers as candidates for the AES. See RSA Laboratories, FAQ 4.0: Frequently Asked Questions About Today's Cryptography: What is the AES? (visited Nov. 29, 1998) < <http://www.rsa.com/rsalabs/faq/html/3-3-1.html> > . For information on the status of AES and the fifteen official candidate algorithms, see generally National Institute of Standards and Technology (NIST), Advanced Encryption Standard (AES) Development Effort (visited Nov. 29, 1998) < http://csrc.nist.gov/encryption/aes/aes_home.htm > .

⁶³ See RSA Laboratories, FAQ 4.0: Frequently Asked Questions About Today's Cryptography: What is the Life Cycle of a Key? (visited Nov. 29, 1998) < <http://www.rsa.com/rsalabs/faq/html/4-1-2-3.html> > (“Each time the key is used, it generates a number of ciphertexts. Using a key repetitively allows an attacker to build up a store of ciphertexts (and possibly plaintexts) which may prove sufficient for a successful cryptanalysis of the key value. Thus keys should have a limited lifetime.”).

2. *Public-key Encryption*

¶ 17 Public-key encryption requires the use of a second independent key to decrypt a message. In a strong public-key system, even knowing the algorithm used and the key used to encrypt the message will not allow recovery of the plaintext.⁶⁴ The basic theory is that one of the keys is published, hence the public key, while the other, the private key, is kept secret. The need for the sender and receiver to share secret information is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared. In this system, it is no longer necessary to trust the security of some means of communication.⁶⁵ The only requirement is that public keys be associated with their users in a trusted or authenticated manner. Anyone can then use the public key to send messages that will be readable only by the private key owner. Needless to say, the security of any public-key system is predicated on keeping the private keys secret. Any failure to do so completely destroys any privacy and potentially renders insecure any messages encrypted with the compromised private key.

¶ 18 A significant disadvantage of using public-key cryptography for encryption is its inferior speed. There are many secret-key encryption methods that are significantly faster than any currently available public-key encryption method. Nevertheless, public-key cryptography can be used with symmetric-key cryptography to combine the security advantages of public-key systems and the speed advantages of secret-key systems; an example of this is the commonly-known digital envelope.⁶⁶

3. *Authentication*

¶ 19 Despite the marvels of private key encryption and the potential advantages of combining both private and symmetric forms of encryption, the end-user's privacy concerns are not yet relieved. Significant problems with authenticating

⁶⁴ See RSA Laboratories, *supra* note 53.

In public-key cryptosystems, the private key is always linked mathematically to the public key. Therefore, it is always possible to attack a public-key system by deriving the private key from the public key. Typically, the defense against this is to make the problem of deriving the private key from the public key as difficult as possible. For instance, some public-key cryptosystems are designed such that deriving the private key from the public key requires the attacker to factor a large number, in this case it is computationally infeasible to perform the derivation.

Id.

⁶⁵ See *id.*

⁶⁶ See note 56 *supra*, and accompanying text.

the source of the communications and the keys themselves await the unwary. In the standard public-key scenario, where public keys are exchanged over a non-secure line, each party is still faced with the challenge of verifying the origin of the public key they have received and preventing some impostor from interposing himself between the two parties. There is no greater reason to trust a message saying “this is my public key” than to trust any other message saying “this is me.”⁶⁷ Barring an offline secure transfer of public keys, which would undermine one of the central advantages of public-key systems, or some other inside fact known only to the message originator, which is not practical for impersonal electronic commerce, some form of certification is necessary to ensure that the parties to a conversation or transaction can verify each other’s identities.

¶ 20 Digital certificates issued by trusted third parties known as Certificate Authorities (CAs) can serve this function. A Certification Authority (CA) is a body, either public or private, that seeks to fill the need for trusted third party services in electronic commerce by issuing digital certificates that attest to some fact about the subject of the certificate.⁶⁸ In the case discussed, the CA could certify that an individual’s public key actually belongs to them. This immediately raises the question of who certifies the CA. To avoid endless certification chains, a government role⁶⁹ has been proposed and in the interim, CAs have adopted a fairly flat certification hierarchy where they self-certify.⁷⁰

¶ 21 As a step in the correction of the authentication problem, the private key owner can create a unique “digital signature” by encrypting a message with his private key. That digital signature can then be decrypted by anyone having his public key, but the fact that the public key decrypts the message to its original plaintext indicates that it could only have been encrypted by the private key owner. Because the private key owner is solely responsible for the security of the

⁶⁷ “Without help from a source external to the Internet communication, either a trusted third party or some ‘out-of-band’ (non-Internet) communication that is reliable, [the recipient] has no way of assuring himself of the authenticity of any e-mailed communication from a stranger, regardless of what it says.” A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 52 (1996).

⁶⁸ See *id.* at 55.

⁶⁹ “The root key would belong to a state or federal agency, and the few CAs that met state licensing requirements would be rewarded with government certification of their root key. These CAs would then certify the root keys of organizations that wished to manage their own certificates. A CA might certify the root key of ABC Corp, which would in turn be used to certify the keys of, for example, the key manager in each corporate division, which in turn would certify the keys of salespeople, purchasing agents and press secretaries.” *Id.* at 56.

⁷⁰ “The few CAs currently in operation have dealt with the absence of an agreed root certification authority by simply signing their own keys and posting the self-certified key on their Web sites. The self-certified key is then mirrored on other computers.” *Id.* at 57.

private key, the risk of compromising the secret key is greatly reduced compared to symmetric encryption, since the private key is never transferred.⁷¹

B. Executive Branch Regulation

¶ 22 The United States government has long been plagued with the uneasy balance between making encryption publicly available to enhance personal privacy and to encourage the development of electronic commerce and the fear that wholesale use of strong encryption will undermine domestic law enforcement and endanger national security.⁷² FBI director Louis Freeh, perhaps the most adamant opponent of permitting the public availability of strong non-recoverable encryption, has frequently argued that electronic intelligence, especially wiretapping, is crucial to effective law enforcement.⁷³ In his words, if the FBI and local police were to lose the ability to tap telephones because of the widespread use of strong cryptography, the “country [would] be unable to protect itself against terrorism, violent crime, foreign threats, drug trafficking, espionage, kidnapping, and other crimes.”⁷⁴

¶ 23 The widespread use of encryption is potentially just as problematic for the United States intelligence community. Two of the most important functions of the National Security Agency (NSA) are the acquisition and decryption of foreign communications and the traffic analysis of foreign communications. The acquisition and decryption function has been the stuff of headlines, from listening to the Soviet President’s telephone calls from his limousine to breaking German codes in World War II. Traffic analysis is the more subtle process of monitoring the sources and recipients of messages, whether readable or not, to discern lines of

⁷¹ Authentication via secret-key systems requires the sharing of some secret and sometimes requires trust of a third party as well. As a result, a sender can repudiate a previously authenticated message by claiming the shared secret was somehow compromised by one of the parties sharing the secret. For example, the Kerberos symmetric-key authentication system, used for network resource management, involves a central database that keeps copies of the secret keys of all users; an attack on the database would allow widespread forgery. See RSA Laboratories, FAQ 4.0: Frequently Asked Questions About Today’s Cryptography: What are the advantages and disadvantages of public-key cryptography compared with secret-key cryptography? (visited Nov. 29, 1998) < <http://www.rsa.com/rsalabs/faq/html/2-1-3.html> > .

⁷² “Unfortunately, the same encryption technology that can help Americans protect business secrets and personal privacy can also be used by terrorists, drug dealers, and other criminals.” Statement of the White House Press Secretary announcing the Adoption of the Voluntary Escrowed Encryption Standard (Feb. 4, 1994) (on file with author).

⁷³ See generally Encryption, Key Recovery, and Privacy Protection in the Information Age: Hearings Before the Senate Comm. on the Judiciary, 105th Cong. (July 9, 1997) (statement of Louis J. Freeh, Director, FBI).

⁷⁴ Louis J. Freeh, Address Before the Executives’ Club of Chicago 8 (Feb. 17, 1994) (transcript available at the FBI).

command. The volume of communications can indicate imminent operations.⁷⁵ Even if it is not possible to immediately decrypt the message, an individual's message traffic can be monitored through traffic analysis in order to determine his communications patterns. In a world where encryption is the exception rather than the rule, it is much easier to determine who has something to hide as the encrypted, and presumably most interesting or highest value, messages stand out. If the time comes when most message traffic is encrypted, it will be impossible to determine which are the most secret messages in real time and the sheer volume of encrypted message traffic will make traffic analysis difficult. In order to stem the rising proliferation of strong encryption, the government has pursued a two-tiered program of export controls and establishing domestic key recovery standards that will now be addressed in turn.

1. *Export Controls*

¶ 24

Perhaps the central lever used by the Clinton Administration to directly control the proliferation of strong encryption and to encourage the development of a worldwide key escrow infrastructure has been the regulation of encryption exports. Prior to December 30, 1996, the State Department, under the authority of the Arms Control Export Act and the International Traffic in Arms Regulations (ITAR), regulated most encryption exports from the U.S. pursuant to an Executive Order, with the goal of preventing foreigners from acquiring encryption strong enough to interfere with traffic analysis or difficult for U.S. intelligence agencies to crack.⁷⁶ The export of encryption is governed by two sets of regulations: the ITAR, which governs inherently military technology, and the Export Administration Regulations (EAR)⁷⁷ that governs dual-use technology. The ITAR takes precedence and encompassed most encryption products in 1996

⁷⁵ See A. Michael Fromkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 747 (1995).

⁷⁶ The ITAR are administered by the Office of Defense Trade Controls in the State Department, which can transfer an export application to the Commerce Department. The statutory authority for the ITAR is the Arms Export Control Act, 22 U.S.C. § 2778 (1988 & Supp. IV 1992).

⁷⁷ The EAR are administered by the Bureau of Export Administration in the Department of Commerce and are generally less demanding than the ITAR. The statutory authority for the EAR, the Export Administration Act of 1979, 50 U.S.C. §§ 2401-2420 (1988 & Supp. IV 1992), lapsed on August 20, 1994. See 50 U.S.C. app. § 2419 (West Supp. 1994). President Clinton issued an executive order requiring that the EAR be kept in force to "the extent permitted by law" under the International Emergency Powers Act (IEPA), 50 U.S.C. §§ 1701-1706 (1988 & Supp. IV 1992). See Exec. Order No. 12,924, 59 Fed. Reg. 43,437 (1994).

and earlier.⁷⁸ Under ITAR, applications to export DES or stronger encryption were routinely denied. Only strong products that lacked the capability of being adapted to encryption or which were designed for specific banking applications received official export clearance.⁷⁹

¶ 25 Prior to 1994, it could take weeks for a company to obtain an export license for encryption products, and each shipment might require a separate license. On February 4, 1994, the State Department announced streamlined export licensing procedures for encryption products designed to substantially reduce administrative delays and paperwork for encryption exports.⁸⁰ For the first time, encryption manufacturers were permitted to ship their products from the United States directly to their customers within approved regions without obtaining individual licenses for each end user. In addition, a goal of two-day turnaround was implemented for many encryption license requests. Ostensibly to alleviate delays and inconvenience for business travelers, the State Department instituted a personal-use exemption permitting U.S. citizens to take encryption products out of the U.S. temporarily for their own personal use without an export license. To further bolster the acceptance of key escrow technology, key escrow encryption products qualified for special licensing arrangements and could be exported to most end users after initial review.⁸¹ These procedural changes did not, however, change the types of equipment controlled by the munitions list and signaled the beginning of preferential treatment for recoverable encryption products over their non-recoverable counterparts.

¶ 26 On August 17, 1995, the Administration announced its proposal to permit the ready export of encryption software, provided that the products used algorithms with key space that did not exceed 64 bits and the key(s) required to decrypt messages/files were escrowed with government-approved private escrow agents.⁸² Under this proposal, products would be reviewed to verify compliance and then transferred to the Commodity Control List administered by the Department of Commerce where the products could be exported under a general

⁷⁸ See Froomkin, *supra* note 75, at 748.

⁷⁹ See *id.* at 749-50.

⁸⁰ See *Encryption—Export Control Reform*, Statement of Dr. Martha Harris, Deputy Assistant Secretary of State for Political-Military Affairs (Feb. 4, 1994) (on file with author).

⁸¹ See *id.*

⁸² This proposal represented a significant shift away from the “Clipper Chip” proposal that attempted to set a single standard for recoverable encryption in the United States. See Elizabeth Corcoran, *White House to Unveil Data Encryption Plan; Export of ‘Scrambling’ Technologies Allowed*, WASH. POST, Aug. 17, 1995, at D8.

license, formerly restricted to 40-bit encryption products.⁸³ The “carrot and stick” approach to key escrow continued in 1996 with the Clinton administration’s initiative for “a worldwide key management infrastructure with the use of key escrow and key recovery encryption items to promote electronic commerce and secure communications while protecting national security and public safety.”⁸⁴ To encourage industry to develop the key management infrastructure, the President’s interim rule permitted the export and reexport of both encryption hardware and software of 56-bit key length DES or equivalent strength under the authority of a License Exception, if the exporter made satisfactory commitments to build and/or market recoverable encryption items and to help build the supporting international infrastructure.⁸⁵ In tandem, the State Department modified the ITAR to remove and transfer to the Commerce Control List (CCL) all cryptographic items except those specifically designed, developed, configured, adapted, or modified for military applications, including command, control, and intelligence applications.⁸⁶

¶ 27

In addition to loosening export controls while leveraging key escrow programs, the Administration has also pursued a market sector-by-sector approach to export controls.⁸⁷ Not surprisingly, this policy began with lifting the ban on the export of strong encryption technology for U.S. companies engaged in banking and other financial services.⁸⁸ The government most recently expanded the sector exemptions to include subsidiaries of U.S. companies world-

⁸³ See Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List, 61 Fed. Reg. 68,572, 68,573 (1996).

⁸⁴ *Id.*

⁸⁵ See *id.* Three companies were quick to accede to the government’s terms in exchange for authorization to export 56-bit encryption technology. One of the companies, Cylink Corp., included optional key recovery that could be turned off or on depending on business requirements or government regulations. See *Three U.S. Companies Win Approval to Export 56-bit Encryption Technology*, 14 INT’L TRADE REP. 209 (1997).

⁸⁶ See Amendment to the International Traffic in Arms Regulations, 61 Fed. Reg. 68,633 (1996). For one opinion on the benefits of transferring control over encryption exports from the State Department to the Commerce Department, see Stewart A. Baker & Peter Lichtenbaum, *Cutting Red Tape on Encryption*, J. COM., Sept. 27, 1996, at 9A (noting that Commerce has procedures and staff in place to avoid delays in the handling of licenses and arguing for continuation of existing State department licenses and for close attention to the role of the Justice Department and the FBI).

⁸⁷ According to Commerce Secretary William Daley, the sector-specific approach was adopted to break up the policy logjam resulting from industry’s call to loosen controls in the face of demands from law enforcement and national security agencies to tighten controls. See *Encryption Export Controls Debate Enters New Phase*, ELECTRONIC MAIL & MESSAGING SYSTEMS, Aug. 7, 1998, available in 1998 WL 8214667.

⁸⁸ See Niles S. Campbell, *Administration OKs Export of Encryption by Banks Engaged in Electronic Commerce*, 2 BNA’S ELECTRONIC INFO. POL’Y & L. REP. 489 (1997) (announcing the authorization of the export of encryption algorithms using any key length and without key recovery to protect financial transactions conducted over electronic networks, as long as those transactions are primarily financial in nature).

wide, insurance companies, strictly defined health and medical sectors, client-server applications (e.g., SSL) and applications tailored to facilitate secure electronic transactions between merchants and their customers.⁸⁹

¶ 28

Recognizing that it is indeed a global market, the Clinton Administration has tried to encourage global support for encryption controls in general and key escrow, specifically. The United States is not the only government concerned with the law enforcement and national security implications of widespread use of strong non-recoverable encryption products.⁹⁰ All countries that produce software with encryption capabilities control exports of those products to some extent, although the control methodologies and licensing practices vary from country to country, and some countries, notably France, Russia, and Israel, also control imports and/or the domestic use of encryption.⁹¹ There is a significant amount of international cooperation in controlling exports of encryption products.⁹² Nevertheless, efforts to convince the Organization for Economic Cooperation and Development (OECD) to embrace guideline language mandating the

⁸⁹ The U.S. subsidiary exemptions would apply in all but 7 designated terrorist nations, while the remaining exemptions would be applicable to the list of countries designated in the earlier banking regulations. All of the exemptions would apply to encryption products of any key length, with or without key recovery. See Summary of Encryption Policy Update (visited Dec. 12, 1998) < <http://www.bxa.doc.gov/Encryption/EncrpolycyUpdate.htm> > .

⁹⁰ "All governments are aware of the adverse impact that the widespread use of strong encryption can have on law enforcement capabilities. Most are considering the use of trusted third parties and/or key escrow as possible mechanisms in this regard." *Administration Frames Encryption Bill but Shows No Flexibility on Exports*, INSIDE U.S. TRADE, Mar. 21, 1997 (quoting U.S. Special Envoy for Cryptography David Aaron).

⁹¹ See Gary G. Yerkey, *Special Report: Export Controls: U.S. Controls on Encryption Software Have Hurt Exporters, Government Finds*, INT'L TRADE REP., Jan. 17, 1996, at 85 (referring to Government Report: A Study of the International Market for Computer Software with Encryption).

⁹² See *id.*

International efforts to restrict unescrowed cryptography may be growing just as the domestic pressure increases to relax export control. Indeed, the phenomena may be related in either of two ways. The combination of the ITAR with the U.S. dominance of the mass-market software industry allowed foreign governments to avoid the cryptography issue. In effect, U.S. export control also functioned as import control for foreign governments. Other countries had less need for an explicit ban on strong consumer cryptography because U.S. firms' dominance of the market for operating systems and other potential applications of cryptography tended to stifle the growth of indigenous competitors. As it becomes increasingly likely that the ITAR will be relaxed, or possibly even eliminated, foreign governments may feel increased pressure to grapple with the cryptography issue. Alternately, the increased interest of some foreign governments in sponsoring international controls on strong cryptography might be the result of a U.S. government effort to jumpstart domestic escrow policy by orchestrating an international clamor for a domestic policy that otherwise would be more difficult to sell.

A. Michael Froomkin, *It Came From Planet Clipper: The Battle Over Cryptographic Key "Escrow"*, 1996 U. CHI. LEGAL F. 15, 60-61.

use of key recovery systems were largely unsuccessful in 1997.⁹³ Rather than mandatory key escrow, the OECD plan focussed on trustworthiness, user choice, national and international standard setting, and respect for individual privacy in the development of national policies.⁹⁴ The Clinton Administration nevertheless considered the OECD guidelines “a victory in its long campaign for key recovery systems.”⁹⁵ 1998 was a better year for the Clinton Administration’s effort to forge an international consensus on key escrow and export controls. Following its limited success with OECD, the United States turned to the 33 signatories to the Wassenaar Arrangement, which limits the export of armaments, as a possible forum to achieve international consensus on limiting export of strong encryption.⁹⁶ Its efforts were rewarded with an agreement for stricter controls on mass-market cryptography passed by the member countries in December 1998.⁹⁷ In most cases, the U.S. until recently permitted only 40-bit encryption software to be eligible for “mass-market” treatment. By contrast, most other Wassenaar members allowed the free export of all mass-market encryption software.⁹⁸ Controls on mass-market software remain a source of heated discourse in the United States.⁹⁹

⁹³ See Lawrence J. Speer, *OECD Approves Cryptography Guidelines; Rebuffs Administration’s Key Recovery Plan*, INT’L TRADE REP., Apr. 2, 1997, at 582.

⁹⁴ See *id.* at 583 (detailing eight central principles to OECD cryptography guidelines).

⁹⁵ *Id.* at 582. The OECD guidelines did permit national key recovery systems, subject to the other principles discussed, *supra*, note 94 and accompanying text. *Id.* at 583.

⁹⁶ The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is an international regime designed to promote communication and cooperation in controlling the transfer of arms and dual-use goods (including cryptography). The arrangement requires participating countries to control cryptography on a statutory or regulatory basis, which may include “forms of licensing” or “the ability to monitor transfers of these items.” Still, exports can occur according to the policies and discretion of the participating country. See Stewart Baker, *Revisiting Wassenaar*, MONDAQ BUSINESS BRIEFING, Jan. 13, 1998, available in 1998 WL 9016651.

⁹⁷ See *33 Nations Agree to Stricter Controls on Cryptography*, COMPUTERGRAM INT’L, Dec. 4, 1998, available in 1998 WL 18863434 (quoting U.S. special envoy for cryptography David Aaron as saying that the agreement “closed a loophole which exempted software that is already widely available”).

⁹⁸ See Baker, *supra* note 96.

⁹⁹ Cryptographer Bruce Schneier believes that in extending export controls to mass market software, these nations have made a serious mistake. “There’ll be less security in the world,” Schneier explained, “more opportunity for fraud, more opportunity for crime. If terrorists are targeting computer systems, it will be easier for them now. The U.S. has always tried to convince other countries that it is their governmental duty to spy on people who are not convicted of anything, but this is the first time the government has said that you must make yourself available for police surveillance.” Schneier says there is a widely held but mistaken belief that cryptography is a tool that criminals use. “Privacy is essential to liberty and democracy,” he said. “[T]o me it’s very scary to see it squandered in such a [manner], to be told: ‘You citizens, we don’t trust you enough to give you privacy.’” *33 Nations Agree to Stricter Controls on Cryptography*, *supra* note 97.

Another area [in] which the practice of other Wassenaar members conflict[ed] with U.S. policy [was] the regulation of Internet distribution of encryption software. Some countries (such as the U.K.) have taken the position that their export controls laws do not permit the control of “intangible” items. Thus, even a non-mass market product, that would be controlled if shipped on a disc, [could] be freely distributed via the Internet to foreign buyers.¹⁰⁰

¶ 29

Members of the Wassenaar Arrangement, which replaced the Cold War COCOM¹⁰¹ as an international export mechanism, said the group wants countries to restrict export of mass-market encryption software of 64 bits or more. Until then, there had been no restrictions on the export of mass-market products. The group also removed all controls for encryption software of 56 bits and smaller and for encryption used in consumer electronics products such as DVD or wireless phones.¹⁰² Not everyone was as pleased as the Clinton administration and the significance of the agreement is already being brought into question.¹⁰³ Industry observers and government officials have cautioned that the agreement only applies to 33 Wassenaar Arrangement signatories, and some countries active in cryptography, such as Israel and China, are left out.¹⁰⁴ Significantly, even the Wassenaar

¹⁰⁰ Baker, *supra* note 96.

¹⁰¹ According to the Americans for Computer Privacy (ACP), in 1991 COCOM de-controlled the export of mass market software, recognizing that it is inherently uncontrollable, whether off the shelf or on the internet. See *ACP Opposes Wassenaar Encryption Restrictions*, ARMED FORCES NEWSWIRE SERVICE, Sept. 16, 1998, available in 1998 WL 17228802.

¹⁰² See *International Export Group Wants New Encryption Ban*, COMM. DAILY, Dec. 4, 1998, available in 1998 WL 10697886.

¹⁰³ See *Americans for Computer Privacy Urge Administration to Lift Controls on 56-Bit Encryption Technology*, BUSINESS WIRE, Dec. 4, 1998 (“If we are trying to create a level playing field in the world of encryption, it won’t happen with an agreement that fails to attract key support of major world players.”); Rebecca Sykes, *Agreement Restricts Encryption Export but Observers Question Strength of International Accord*, INFOWORLD, Dec. 14, 1998, available in 1998 WL 21922089 (“The Wassenaar Arrangement calls for member countries to pass local legislation—at their discretion—if they want its provisions to take effect, said Barry Steinhardt, executive director of the Electronic Frontier Foundation, in San Francisco. But it is not clear whether the new part of the agreement will let countries pass legislation at their discretion as normal, or whether it is mandatory. If the new controls are not mandatory, then nothing has changed, because most of the signatories have well-established policies that permit the unfettered export of encryption.”).

¹⁰⁴ See *Encrypt Controls to Expand; 32 Nations to Join U.S. on Export Curbs; Valley Seen Helped*, SAN JOSE MERCURY NEWS, Dec. 4, 1998, at C1, available in 1998 WL 8878222. The fact that the Wassenaar Agreement has no enforcement authority has led to concern by privacy groups that any control regime agreed on by the member countries amounts to nothing more than permission for a unilateral U.S. control against American companies. *ACP Opposes Wassenaar Encryption Restrictions*, *supra* note 101 (noting that the Clinton administration is among the leading proponents of efforts to strictly curtail encryption technology).

Arrangement falls well short of the current U.S. encryption controls¹⁰⁵ and the congressional response has been less than enthusiastic.¹⁰⁶

2. *Key Escrow*

¶ 30

The government's attempts to impose key escrow on the U.S. encryption industry have a long and less than distinguished history. As mentioned in Part III.A.1., government involvement dates to the designation of DES as the U.S. encryption standard in 1977, a decision that was not without controversy.¹⁰⁷ The first attempt at "voluntary" key escrow was the "Clipper Chip" initiative, announced by the Clinton Administration in 1993 as "a voluntary program to improve the security and privacy of telephone communications while meeting the legitimate needs of law enforcement."¹⁰⁸ The Clipper Chip was billed as a state of the art microchip developed by government engineers that could be used in relatively inexpensive encryption devices attached to an ordinary telephone to scramble telephone conversations using an algorithm more powerful than many in commercial use at the time.¹⁰⁹ One major catch to the government's illustrious

¹⁰⁵ See Robert MacMillan, *Germany, Japan, UK Will Tighten Encryption Controls*, NEWSBYTES NEWS NETWORK (Dec. 3, 1998), available in 1998 WL 20719774 ("[T]he U.S. government's praise is directed at a policy that still is less restrictive than its own," said Business Software Alliance (BSA) Policy Manager Anne Gavin).

¹⁰⁶ Senate Communications Subcommittee Chairman Burns (R-Mont.), who has sponsored legislation to allow wider use of encryption, said: "It is still baffling to people like me who view the Internet as an information revolution that should be allowed to grow and flourish that the Clinton-Gore Administration would work consistently to thwart the security backbone of electronic commerce and computer privacy." He said the Administration "continues to live in this mythical world in which turning back the tide on technology and privacy is the policy tool of choice. If they think that getting a few countries to agree to their restrictions is going to get the job done in the Digital Age, they're farther down the primrose path than I thought." *International Export Group Wants New Encryption Ban*, *supra* note 102.

¹⁰⁷ See Froomkin, *supra* note 75, at 736-37 ("The designation of DES as the U.S. standard was controversial, foreshadowing the current controversy over Clipper. An earlier version of the IBM project used a key with well over one hundred bits. The key shrank to fifty-six bits by the time it became the U.S. standard. Critics charged that the shortened key was designed to be long enough to frustrate corporate eavesdroppers, but short enough to be broken by the NSA. Some critics also feared there might be a "back door," an implanted weakness in a key part of the encryption algorithm known as S-boxes, that would allow the agency to use computational shortcuts to break the code.")

¹⁰⁸ Statement by White House Press Secretary Announcing Clipper Chip Initiative (April 16, 1993) (on file with author).

¹⁰⁹ See *id.* The Clipper Chip utilized a symmetric 64-bit block encryption algorithm called "Skipjack" which used 80 bit keys (compared with 56 for DES) and thirty-two rounds of scrambling (compared with sixteen for DES). Using an assumption that the cost of processing power is halved every eighteen months, the review board convened by NIST to evaluate SKIPJACK concluded that it would be thirty-six years before the cost of breaking SKIPJACK would be equal to the cost of breaking DES, there was no significant risk that SKIPJACK would be broken by exhaustive search in the next thirty to forty years, and there was no significant risk that SKIPJACK could be broken through a shortcut method of attack. See Ernest F. Brickell et al., *SKIPJACK Review Interim Report: The SKIPJACK Algorithm 1* (July 28, 1993).

design was the built-in key recovery scheme.¹¹⁰ To prevent the development of devices that interoperated with “legitimate” SKIPJACK devices but failed to implement the law enforcement access field (LEAF) which enabled an authorized law enforcement official to recover the session key, in short, non-recoverable Clipper Chips, the underlying SKIPJACK algorithm was classified SECRET—NOT RELEASABLE TO FOREIGN NATIONALS.¹¹¹ While the administration emphasized the fact that the “Clipper Chip” provided law enforcement with no new authorities to access the content of the private conversations of Americans, there was also no additional requirement above a legal wiretap authorization to obtain the two keys necessary to listen to the unencrypted conversation.¹¹² An interesting insight into the Clinton Administration’s view of the private use of encryption was provided when the White House was asked if it would use legal means to restrict access to more powerful encryption devices if a technological solution such as the Clipper Chip were unavailable.

This is a fundamental policy question which will be considered during the broad policy review. The key escrow mechanism will provide Americans with an encryption product that is more secure, more convenient, and less expensive than others readily available today, but it is just one piece of what must be the comprehensive approach to encryption technology, which the Administration is developing.

The Administration is not saying, “since encryption threatens the public safety and effective law enforcement, we will prohibit it outright” (as

¹¹⁰ Each device containing the chip was to have two unique keys that would be needed by authorized government agencies to decode messages encoded by the device. The two keys were intended to be deposited separately in two “key-escrow” data bases that were to be established by the Attorney General. *See id.*

¹¹¹ *See* Brickell et al., *supra* note 109 (“While the internal structure of SKIPJACK must be classified in order to protect law enforcement and national security objectives, the strength of SKIPJACK against a cryptanalytic attack does not depend on the secrecy of the algorithm.”).

¹¹² The official questions and answers that accompanied the White House Press release announcing the Clipper Chip provided the following illuminating example.

Q: Suppose a law enforcement agency is conducting a wiretap on a drug smuggling ring and intercepts a conversation encrypted using the device. What would they have to do to decipher the message?

A: They would have to obtain legal authorization, normally a court order, to do the wiretap in the first place. They would then present the documentation of this authorization to the two entities responsible for safeguarding the keys and obtain the keys for the device being used by the drug smugglers. The key is split into two parts, which are stored separately in order to ensure the security of the key escrow system.

Questions and Answers About the Clinton Administration’s Telecommunications Initiative, following Statement by White House Press Secretary Announcing Clipper Chip Initiative (April 16, 1993) (on file with author).

some countries have effectively done); nor is the U.S. saying that “every American, as a matter of right, is entitled to an unbreakable encryption product.” There is a false “tension” created in the assessment that this issue is an “either-or” proposition. Rather, both concerns can be, and in fact are, harmoniously balanced through a reasoned, balanced approach such as is proposed with the “Clipper Chip” and similar encryption techniques.¹¹³

¶ 31 The following year, the combination of SKIPJACK and the Clipper Chip was announced by NIST as the Escrowed Encryption Standard (EES), a voluntary Federal Information Processing Standard, to enable government agencies to purchase the Key Escrow chip for use in telephones and modems.¹¹⁴ The escrow agents named by the Attorney General for EES were NIST in the Department of Commerce and the Automated Systems Division of the Department of the Treasury.¹¹⁵ Detailed procedures for the handling of the keys were also promulgated.¹¹⁶

¶ 32 After the adoption of the Clipper Chip Standard, the Clinton Administration progressively loosened export controls for encrypted products while favoring recoverable products and using the export control regulations as a tool both explicitly and implicitly to encourage the development of a key recovery infra-

¹¹³ *Id.*

¹¹⁴ See Statement of the White House Press Secretary Announcing the Adoption of the Voluntary Escrowed Encryption Standard, *supra* note 72. For the actual EES standard, see Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard, 59 Fed. Reg. 5997 (1994).

¹¹⁵ See *Attorney General Makes Key Escrow Encryption Announcements*, Attorney General Press Release (Feb. 4, 1994) (on file with author).

¹¹⁶ See *id.*:

When an authorized government agency encounters suspected key-escrow, a written request will have to be submitted to the two key escrow agents. The request will, among other things, have to identify the responsible agency and the individuals involved; certify that the agency is involved in a lawfully authorized wiretap; specify the wiretap’s source of authorization and its duration; and specify the serial number of the key-escrow encryption chip being used. In every case, an attorney involved in the investigation will have to provide the escrow agents assurance that a validly authorized wiretap is being conducted.

Upon receipt of a proper request, the escrow agents will transmit their respective key components to the appropriate agency. The components will be combined within a decrypt device, which only then will be able to decrypt communications protected by key-escrow encryption. When the wiretap authorization ends, the device’s ability to decrypt communications using that particular chip will also end.

For a more detailed discussion of the proposed procedures for release of the keys, see *Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to Title III*, U.S. Department of Justice Press Release (Feb. 4, 1994); *Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to FISA*, U.S. Department of Justice Press Release (Feb. 4, 1994); *Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to State Statutes*, U.S. Department of Justice Press Release (Feb. 4, 1994) (all on file with author).

structure. With the September 1998 revisions to the export control regulations, the Administration lifted the requirement for key recovery in order to export 56-bit encryption products.¹¹⁷ Favoritism for recoverable products continued, however, as the new regulations permit exports, under Export Licensing Arrangements, of recoverable products of any key length to foreign commercial firms for internal, company-proprietary use in a designated list of countries.¹¹⁸ The export controls also continue to bar the export of strong non-recoverable encryption to individual consumers.¹¹⁹

C. Legislative Responses

¶ 33

The Congress has by no means stood idly by as the encryption debate has evolved. A number of bills have been introduced, none of which has resulted in legislation regulating export controls or key escrow. The first of the bills introduced in 1997, was H.R. 695, the “Security and Freedom Through Encryption (SAFE) Act.” Following its introduction on February 12, 1997, the SAFE bill appeared to enjoy wide bipartisan support in the House of Representatives, including the critical Judiciary Committee which held primary jurisdiction. The bill proposed that, except in the furtherance of a crime, any person within the U.S. and any U.S. person abroad may use any encryption algorithm, any key length, and any implementation.¹²⁰ SAFE thus became the first bill to explicitly include freedom from domestic regulation as well as a provision barring mandatory key escrow, although it did provide for law enforcement access to encrypted information when authorized by law.¹²¹ The SAFE bill also differed considerably from the Administration policy on export controls. It provided that licenses would not be required for encryption software, regardless of key length, that is generally available to the public and designed for installation by the purchaser/user, so called “off-the-shelf” items.¹²² The end result would have been to make robust encryption freely available to all but embargoed destinations. The

¹¹⁷ See *Summary of Encryption Policy Update*, *supra* note 89. (“Hardware and software exports of up to ‘56 bits DES and equivalent’ products will be eligible for license exception treatment to all users and destinations (except the seven State supporters of terrorism) after a one-time technical review.”).

¹¹⁸ See *id.*

¹¹⁹ See *id.*

¹²⁰ See H.R. 695, 105th Cong. § 2 (1997).

¹²¹ The bill did not specify how law enforcement access would be implemented or controlled. See *id.*

¹²² See H.R. 695 § 3.

bill passed the Judiciary Committee by voice vote and 43 members of the House sent a letter to President Clinton calling for the President to lift the export restrictions on encryption technology.¹²³ The FBI and other law enforcement agencies lobbied heavily against the SAFE Bill and Rep. Oxley (R., Ohio) tried and failed in the Commerce Committee to add an amendment that would have required all encryption products to include a backdoor allowing government access to otherwise secure computer files and communications.¹²⁴ No final action was taken by the 105th Congress.¹²⁵

¶ 34

The Senate responded on February 27, 1997, by introducing a pair of encryption bills, S. 376, the “Encrypted Communications Privacy Act of 1997”, also known as the Burns Bill and S. 377, the “Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1997”, also known as the Leahy Bill. S. 376 addressed both domestic use and export controls of encryption technology. On the domestic front, the bill affirmed the right of any person in the U.S. or U.S. citizen abroad to use any type, strength, or implementation of encryption technology.¹²⁶ The bill prohibited mandatory key escrow and was the first legislation to give detailed guidance regarding duties of key holders and limits on the use of released keys.¹²⁷ Similar to SAFE, S. 376 proposed to make generally available encryption products freely exportable, without regard to key length or algorithm.¹²⁸ If possible, S. 377 or Pro-CODE took an even more aggressive approach, including a laundry list of seventeen findings detailing the many reasons why strong encryption is critical to American business competitiveness and why the regulatory efforts to date were flawed and misguided.¹²⁹ Most notably, the findings declared that “[t]he regulatory efforts . . . to promulgate standards and

¹²³ See Elizabeth Corcoran, *House Committee Approves Bill to Relax Curbs on Encryption*, WASH. POST, May 15, 1997, at E1.

¹²⁴ See Rajiv Chandrasekaran, *Decoding Provision Defeated; House Panel Rejects FBI Software Proposal*, WASH. POST, Sept. 25, 1997, at E2.

¹²⁵ The Judiciary Committee and the International Relations Committee reported out versions similar to the Commerce Committee while the Select Committee on Intelligence and the National Security Committee produced radically different versions which mandated the domestic controls rejected by the Commerce Committee. See *Telecom Industry Keeps Closer Eye on Encryption Bills, Opposes Domestic Controls*, TELECOMMUNICATIONS REP., Sept. 29, 1997, at 14.

¹²⁶ See S. 376, 105th Cong. § 5 (1997).

¹²⁷ In addition to providing criminal penalties for the unauthorized release of the key, the bill limited authorized release to with the consent of the key owner, as required to provide service, or release to law enforcement with a Title III warrant for wire or electronic communications in real time or an ECPA warrant for stored electronic communications. See S. 376 § 6.

¹²⁸ See *id.*

¹²⁹ See S. 377, 105th Cong. § 2 (1997).

guidelines in support of government-designed solutions to encryption problems that were not developed in the private sector and have not received widespread commercial support have had a negative impact on the development and marketing of products with encryption capabilities by United States businesses.” The Administration’s Clipper Chip initiative was likewise characterized as “flawed and controversial.”¹³⁰ Not surprisingly, Pro-CODE expressly prohibited the Secretary of Commerce from mandating standards for the commercial encryption industry and included provisions for the free sale of encryption products in the U.S. and a prohibition on mandatory key escrow, similar to the SAFE bill.¹³¹ Pro-CODE lacked the detailed instructions for implementing voluntary key escrow present in S. 376, but did propose removing export controls on generally available encryption products, using language similar to SAFE and S. 376.¹³² At the close of the 105th Congress, neither S. 376 nor S. 377 had been the subject of a floor vote, averting a potential Presidential veto.¹³³

¶ 35

Despite the significant similarities among the preceding three bills, the Administration was not yet prepared to passively witness the demise of its carefully wrought encryption policy. In response, the Administration proposed the “Electronic Data Security Act of 1997” which focused on the domestic use of encryption and specifically found that “the lack of a key management infrastructure impedes the use of cryptography and, therefore, the potential of electronic commerce.”¹³⁴ The draft legislation gave considerable insight into the Administration’s vision of an effective key management infrastructure including registration of certificate authorities and recovery agents and release of recovery information by key recovery agents. Despite its clear leanings in favor of key escrow, the proposal did explicitly state that participation in key escrow was voluntary and did permit within the U.S. the use of any encryption method, regardless of algorithm or key length. Predictably, the Administration proposal avoided any mention of export controls, signaling continued opposition to further liberaliza-

¹³⁰ *Id.*

¹³¹ *See* S. 377 § 5.

¹³² *See id.*

¹³³ While many members of the Senate Commerce Committee expressed skepticism that the Administration plan balances industry needs with those of law enforcement, few signaled outright support for the Leahy or Burns proposals. *See Administration Frames Encryption Bill but Shows no Flexibility on Exports*, *supra* note 90 (“[T]here is no sense in passing a bill that the President will veto,” said Commerce Committee Chairman John McCain (R-Az.).”).

¹³⁴ Text of Administration March 12 Key Recovery Draft Legislation (Mar. 12, 1997) < http://www.cdt.org/crypto/970312_admin.html > .

tion.¹³⁵ As a result, the proposal drew sharp attacks from the primary sponsor of the SAFE bill, Hon. Bob Goodlatte (R-Va.), who called the plan “an Industrial Age solution to an Information Age problem.” Congressman Goodlatte focussed on the need to provide for more expeditious increases in overall Internet security, and to ensure that American exporters are not placed at a competitive disadvantage with respect to encryption technology producers overseas. He was perhaps the first to characterize the Clinton plan as the “technological equivalent of mandating that the government be given a key to every home in America.”¹³⁶ The Administration proposal failed to garner a congressional sponsor but did significantly influence the next major congressional action.

¶ 36

Evidence that not all of the Administration’s suggestions had fallen on deaf congressional ears was provided by the next legislative attempt to create a workable solution to the encryption impasse, S. 909, the Secure Public Networks Act (SPNA), also known as the McCain-Kerrey Bill.¹³⁷ SPNA represented a significant departure from the prior congressional legislation and a major shift towards the Administration’s proposed legislation.¹³⁸ The bill establishes a regulatory framework for key recovery agents and certificate authorities. The bill does state, however, that it will be lawful for any person in the U.S. to use any encryption regardless of algorithm or key length, and the government is prohibited from requiring the third party escrow of keys used for the encryption of communications between private parties within the U.S. The bill also contains some modest export liberalization.¹³⁹ Expedited review procedures were proposed for certain

¹³⁵ William Reinsch, Undersecretary of Commerce, stated that “the Administration cannot support” the SAFE bill since it “proposes export liberalization far beyond what the Administration can entertain.” The Administration was also fearful that the passage of the SAFE Bill would preclude the development of voluntary key recovery. *Hearings on Administration Encryption Policy Before the Subcomm. on Courts and Intellectual Property of the House Judiciary Comm.*, 105th Cong. (Mar. 20, 1997), available in 1997 WL 138509 (F.D.C.H.) (Testimony of Honorable William A. Reinsch, Under Secretary of Commerce). Undersecretary Reinsch also testified before the Senate that the Administration would be unable to support either S. 376 or S. 377. *Hearing on Legislation That Would Delineate Encryption Protocol for Online Entities Before the Senate Commerce, Science and Transportation Comm.*, 105th Cong. (Mar. 19, 1997), available in 1997 WL 128216 (F.D.C.H.) (Testimony of Honorable William A. Reinsch, Under Secretary of Commerce).

¹³⁶ Hearings on The Security and Freedom Through Encryption (SAFE) Act of 1997 Before the Subcomm. On International Economic Policy and Trade of the House International Relations Comm., 105th Cong. (May 8, 1997) (Prepared Statement of Rep. Bob Goodlatte (R-Va.)).

¹³⁷ See S. 909, 105th Cong. (1997).

¹³⁸ For a useful comparison between S. 909 and the Administration draft legislation, see CDT Analysis of the McCain-Kerrey Bill (June 17, 1997) (noting that “the McCain-Kerrey bill actually goes even further than the Administration bill in forcing the domestic and worldwide adoption of key recovery systems.”) < http://www.cdt.org/crypto/legis_105/mccain_kerrey/analysis.html > .

¹³⁹ Encryption products up to 56 bits, and key recovery products (without regard to algorithm or key length), will be exportable under a license exception, following a one-time review. See S. 909 §§ 302, 304. Other encryption products (i.e. non-recovery products greater than 56 bits) can qualify for individual

industry sectors, similar to the Administration export regulations later implemented in September 1998, for exports involving banks, financial institutions, health care providers, and subsidiaries of U.S. companies.¹⁴⁰ The Commerce Secretary would be authorized to prohibit any export if he or she, in consultation with other agencies, finds that the encryption product would be used against the national security, diverted to military, terrorist, or criminal use, or re-exported without authorization.¹⁴¹ Perhaps most controversial is the bill's provision for the "voluntary" registration of key recovery agents and certificate authorities,¹⁴² which encourages registration by providing liability benefits for registered entities.¹⁴³ Once registered, a certificate authority is prohibited from issuing a public-key certificate to a person unless that person (1) stores key recovery information with a registered key recovery agent or (2) makes other arrangements that ensure lawful and confidential access to this information.¹⁴⁴ A key recovery agent, whether registered or not, must disclose recovery information to a government entity when that entity has a subpoena which is based upon some independent lawful authority to obtain the underlying encrypted data.¹⁴⁵ The key recovery agent is required to keep confidential all requests for such information.¹⁴⁶ Although the "Secure Public Networks Act" was introduced as a compromise, there appears to be little enthusiasm for it among the backers of SAFE and Pro-CODE.

¶ 37

In the second session of the 105th Congress, the Ashcroft-Leahy-Burns E-Privacy Act ("Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace") was introduced in another attempt to break the impasse.¹⁴⁷ The bill includes both significant privacy protections and relaxed export controls to aid U.S. business while providing significant advantages to law enforcement over all but the SPNA bill. The bill allows Americans to buy and sell any strength of encryption they desire.¹⁴⁸ It applies the same privacy protections to

licenses. Factors to be considered include whether the product is a generally available mass-market product, and whether the product or products of similar strength are available in the country to which the product would be exported. See S. 909 § 307.

¹⁴⁰ See S. 909 § 305.

¹⁴¹ See S. 909 § 306.

¹⁴² See S. 909 § 401.

¹⁴³ See S. 909 §§ 501-504.

¹⁴⁴ See S. 909 § 405.

¹⁴⁵ See S. 909 § 406.

¹⁴⁶ See S. 909 § 403.

¹⁴⁷ See S. 2067, 105th Cong. (1998).

¹⁴⁸ See S. 2067 § 101.

encryption that currently apply to other records in an individual's possession.¹⁴⁹ It allows the export of "mass-market" encryption, which is deemed uncontrollable given the volume sold and ease of distribution, as well as certain hardware and software when comparable foreign products are deemed available.¹⁵⁰

¶ 38 For the benefit of law enforcement, the bill establishes a National Electronic Technologies ("NET") Center, which would assist law enforcement at all levels with expertise in encryption technology, similar to the "Information Security Board" established in Pro-CODE.¹⁵¹ The bill subjects all encryption products to a technical review of their capabilities prior to export.¹⁵² In addition, it conditions the export of "non mass-market" encryption products upon a determination of foreign availability by a government-industry board.¹⁵³ While the bill prohibits the mandatory escrow of decryption keys,¹⁵⁴ it extends the current ECPA standard to encryption keys by permitting law enforcement access to decryption keys under existing wiretap authority and allowing them to obtain keys or third-party assistance for remotely stored data with a court order or subpoena.¹⁵⁵ The bill creates a criminal offense for the use of encryption to conceal incriminating evidence pertaining to the commission of a felony.¹⁵⁶ While the E-Privacy act has garnered significant support from privacy groups,¹⁵⁷ it had not made it to a floor vote in the Senate as of the end of the 105th Congress.

¶ 39 The SAFE Bill was reintroduced in the 106th Congress¹⁵⁸ and was passed by a unanimous voice vote without amendment by the House Judiciary Subcommittee on Courts and Intellectual Property.¹⁵⁹ By the end of the 105th Congress

¹⁴⁹ See S. 2067 § 103 (amending Section 2703 of title 18, United States Code to allow government access to "the contents of an electronic record in networked electronic storage only if the person who created the record is accorded the same protections that would be available if the record had remained in that person's possession.").

¹⁵⁰ See S. 2067 §§ 302, 305.

¹⁵¹ See S. 2067 § 201.

¹⁵² See S. 2067 § 302.

¹⁵³ See S. 2067 § 305.

¹⁵⁴ See S. 2067 § 101.

¹⁵⁵ See S. 2067 § 201.

¹⁵⁶ See S. 2067 § 201.

¹⁵⁷ See, e.g., Senators Introduce Pro-Privacy Encryption Bill, in Stark Contrast to Administration Position, CDT POLICY POST (The Center for Democracy and Technology, Washington, D.C.), Volume 4, Number 11 (1998) < http://www.cdt.org/publications/pp_4.11.html > .

¹⁵⁸ See H.R. 850, 106th Cong. (1999).

¹⁵⁹ See SAFE Act (HR 850) Passes Subcommittee by Unanimous Voice Vote (visited Mar. 15, 1999) < <http://www.cdt.org/crypto/> > .

(1997-98), the SAFE bill had 249 co-sponsors in the House. The bill was reported with widely divergent amendments by 5 committees: Judiciary, International Relations, National Security, Intelligence, and Commerce, and was not brought before the full House for a vote, partly because of the opposition of then-Rules Committee Chairman Gerald Solomon (R-NY). Solomon has retired and SAFE Act co-sponsor David Dreier (R-CA) now chairs the Rules Committee.¹⁶⁰ In addition, Senator Conrad Burns (R-MT) has announced plans to introduce in the Senate similar legislation lifting encryption export controls.¹⁶¹ Without decisive congressional action in passing the SAFE bill or comparable legislation, as will be argued for in Parts V & VI, *infra*, the Commerce Department regulations will likely remain as the principle manifestation of the U.S. government's policy on encryption.

D. *The Industry Response—“Private Doorbell”*

¶ 40

For more than five years, the high-tech industry fought the ban on encryption exports with only marginal and incremental success. Despite the support it has managed to garner in Congress, the industry has found the FBI and NSA its most adamant opponents due to lingering security concerns.¹⁶² Since the initial proposal of the Clipper Chip, the Clinton Administration has liberalized export controls to a limited degree but has remained committed to key escrow and developing a worldwide infrastructure.¹⁶³ In an apparent concession to the Administration's continued emphasis on law enforcement access to plaintext messages, a consortium of 13 high-technology vendors came out in support of a “private doorbell” system as a means to end the current stalemate over U.S. businesses' right to export high-level 128- and 256-bit key encryption.¹⁶⁴ This “private doorbell” approach to encryption products ensures privacy while responding to the concerns of law enforcement authorities. Information traveling over a data network remains secure and private unless a network operator is served with a legal warrant or court order to give access to law enforcement. In no case does law enforcement obtain access to data without the knowledge of the

¹⁶⁰ See *Background on Encryption Fight*, CDT POLICY POST (The Center for Democracy and Technology, Washington, D.C.), Vol. 5, No. 4 (1999) < http://www.cdt.org/publications/pp_5.4.html > .

¹⁶¹ See *id.*

¹⁶² See John Simons, *U.S. to Allow Coalition of Companies to Export New Encryption Technology*, WALL ST. J., Oct. 19, 1998, at B5.

¹⁶³ See *supra* Part III.B.

¹⁶⁴ See Laura DiDio, *Vendors Support 'Private Doorbell' ...*, COMPUTERWORLD, July 20, 1998, at 14.

systems administrator.¹⁶⁵ Particularly significant from the standpoint of industry and privacy groups, the private doorbell requires no key recovery infrastructure.¹⁶⁶ Despite the absence of conventional key escrow, the Commerce Department approved the export of 56-bit DES products, including most firewalls, VPNs (Virtual Private Networks), and E-commerce products, to virtually all customers and countries, and those products with stronger levels of encryption to commercial end users in certain countries, hailing the result as “an excellent example of the ability of government and the private sector to partner to find solutions to the encryption issue.”¹⁶⁷ The extent of the Commerce Department’s acceptance of this new concept as a viable alternative to key recovery is evident in the revised definition of “recoverable products” included in the September 1998 revisions to the export control regulations.

A product or system designed such that network administrator or other authorized persons who are removed from the end user can provide law enforcement access to plaintext without the knowledge or assistance of the end user. This includes, for example, products or systems where plaintext exists and is accessible at intermediate points in a network or infrastructure system, enterprise-controlled recovery systems, and products which permit recovery of plaintext at the server where a system administrator controls and/or can provide recovery of plaintext across an enterprise, and so on.¹⁶⁸

The industry considered the approvals a strong first step but only a single step in the ongoing process of liberalizing export controls on encryption.¹⁶⁹

¹⁶⁵ See *The Alliance for Network Security Praises Encryption Export Approval as Good First Step*, BUS. WIRE, Oct. 19, 1998. The “private doorbell” system allows data to be kept private while giving law enforcement restricted access to an entire message at the beginning and end of network data transmissions. These “private doorbell” access points rest inside “routers,” the hardware that ushers data through small and large networks. The doorbell can also be in software programs that control networks. An administration official said the technology is helpful to law enforcement because it allows them access to e-mail systems, which have proved the most difficult to monitor. Simons, *supra* note 162.

¹⁶⁶ “It proves that market responses to customer demand can help meet the needs of law enforcement, without infringing on the privacy rights of all Americans.” Mary Mosquera, *Encryption Plan Lets United States Compete*, CMP TECHWEB, July 13, 1998, available in 1998 WL 9297015 (quoting Ed Gillespie, ACP Executive Director).

¹⁶⁷ “We are optimistic that the industry will be able to build on this market-driven solution to further expand its world market share.” *The Alliance for Network Security Praises Encryption Export Approval as Good First Step*, BUS. WIRE, Oct. 19, 1998 (quoting Under Secretary of Commerce for Export Administration, William A. Reinsch).

¹⁶⁸ *Summary of Encryption Policy Update*, *supra* note 89.

¹⁶⁹ The industry still plans to push to broaden the rules. Companies are still forbidden, for instance, from selling the new products to foreign telecommunications companies and Internet service providers. Coalition members said they want those exemptions eliminated, especially since European companies can freely sell to telecommunications firms and Internet service providers. Even so, the new compromise “is

¶ 41 Of potentially even greater significance to the ongoing encryption debate, the wide acceptance of the “private doorbell” system may moot one of the issues that divides private industry and law enforcement: real-time decryption.

Law enforcement has pressed hard for the industry to develop the capacity to decrypt scrambled messages as they pass over the Internet. Industry has resisted. If the private doorbell becomes a reality, the argument for real-time decryption loses much of its force.

Materials move so rapidly in cyberspace that the justification for real-time access no longer holds water. If critical material can be collected at either end, what difference will a few minutes (or less) make?¹⁷⁰

¶ 42 Under certain scenarios, however, the approach might not work to provide law enforcement access to plaintext messages. For example, if two parties encrypted their messages before sending them, as is often the case, the intercepted traffic would be impossible to decipher. So-called end-to-end encryption is widely available. “There are limits to what this technology can do,” said an executive with one of the member companies. “This is a lock on a door, but there will need to be other locks on doors, as well, to achieve the kind of security we want.”¹⁷¹

IV. IS KEY RECOVERY CONSTITUTIONAL?

¶ 43 In considering the constitutionality of any potential encryption recovery scheme, the constraints of the Fourth and Fifth Amendments must be analyzed. The following section will illustrate that these Amendments do little to constrain the government’s previously proposed key escrow scheme and less to restrict the deployment of “private doorbell” systems advocated by industry to satisfy export control regulations. While the Fourth and Fifth Amendments are central to the Bill of Rights’ guarantees of privacy from government intrusion and freedom from compulsory self-incrimination, they do little, as currently interpreted, to protect the lawful use of strong non-recoverable encryption by individuals. Nor do they require government to justify the need for back door access to strong

a policy middle ground,” said Dan Scheinman, vice president of legal and government affairs for Cisco Systems. “Right now the international market for encryption is fragmented, and American companies have been shut out. This gives us a foothold in the market, our chance to try and compete.” Simons, *supra* note 162.

¹⁷⁰ Emily Frye, *When the Law Rings a Private Doorbell, Who Answers?*, COMPUTERWORLD, Sept. 14, 1998, at 25.

¹⁷¹ Ralph T. King Jr. & John Simons, *New Encryption Method May Break Impasse in U.S.*, WALL ST. J. EUR., July 14, 1998, at 6, available in 1998 WL-WSJE 12733258.

encryption products or to show that the regulatory measures are narrowly tailored to meet the stated objectives of preventing criminal and terrorist use of strong, non-recoverable encryption. The ensuing constitutional analysis will seek to show how key recovery legislation could be structured to satisfy the Fourth and Fifth Amendments. This analysis should not be construed to be a normative judgement in favor of key recovery, but rather an illustration of the inadequacies of the current Supreme Court interpretations of these Amendments in protecting the ability to use strong encryption to preserve personal privacy.

A. *The Courts May Interpret the Fourth Amendment to Exempt Key Recovery from Protection at the Threshold*

¶ 44

The Fourth Amendment protects “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” It also provides that “no Warrants shall issue, but upon probable cause” and “particularly describing” the objects of search or seizure.¹⁷² The reasonableness and warrant requirements help to ensure that, under our system of government, law enforcement officials will not engage in dragnets or general searches, no matter how useful they might be in facilitating occasional access to evidence of crimes.¹⁷³ One of the significant concerns is that the search, especially a general one, sweeps in much that is not criminal behavior and that is profoundly personal. The requirement to turn over one’s encryption key, *a priori* and without any prior showing of probable cause to believe criminal conduct has taken or will take place, would seem to implicate this most fundamental concern of the Fourth Amendment. While the complete lack of prior criminal conduct would seem determinative of whether the Fourth Amendment has been violated, the legal precedent as it exists today mandates a fairly technical threshold analysis to determine if the bedrock principles of the Fourth Amendment are even applicable to the conduct in question. The real threat to privacy interests is that the courts will misapprehend the nature of the technology and will therefore miscategorize key escrow to place it outside the ambit of the Fourth Amendment.

¹⁷² U.S. CONST. amend. IV.

¹⁷³ See Privacy in a Digital Age: Encryption and Mandatory Access: Hearings Before the Subcomm. on the Constitution, Federalism, and Property of the Senate Judiciary Comm., Mar. 17, 1998 (Prepared statement of Professor Kathleen Sullivan, Stanford Law School) (visited Mar. 6, 1999) < <http://www.computerprivacy.com/archive/03171998-2.shtml> > .

1. *Government Action*

¶ 45 The Fourth Amendment, like the remaining Bill of Rights protections, applies only to government searches.¹⁷⁴ The Supreme Court held in *Coolidge v. New Hampshire* that if a private citizen “wholly on [his] own initiative” turns over certain articles to the police for use in a criminal investigation, “there can be no doubt under existing law that the articles would later [be] admissible in evidence.”¹⁷⁵ While this may seem a truism, its application to key recovery schemes can become fairly subtle depending on the degree of government involvement, the level of government coercion of private individuals and industry to participate in the key recovery plan, and what the government intends to do with the keys or access to the plaintext messages that have been previously lawfully obtained by private parties.

¶ 46 For the purposes of the Fourth Amendment, the Supreme Court has adopted a much broader definition of government action than just the traditional search pursuant to a criminal investigation by police. The Supreme Court has recognized the intrusive nature of various regulatory searches conducted by government officials, holding that it would be “anomalous to say that the individual and his private property are fully protected by the Fourth Amendment only when the individual is suspected of criminal behavior.”¹⁷⁶ The Court has used similar logic to extend the Fourth Amendment to searches by other government employees who do not typically function in a law enforcement capacity including fire inspectors,¹⁷⁷ OSHA inspectors,¹⁷⁸ and federal mine inspectors.¹⁷⁹ Considering the broad scope of whom has been considered to be a government official, it is likely that if a key recovery plan involved collection of encryption keys or controlled access to plaintext messages prior to encryption or after decryption by

¹⁷⁴ See *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921) (The Fourth Amendment was “intended as a restraint upon the activities of sovereign authority and was not intended to be a limitation upon other than government agencies.”).

¹⁷⁵ 403 U.S. 443, 487 (1971). See also *Walter v. United States*, 447 U.S. 649, 656 (1980) (“[A] wrongful search or seizure conducted by a private party does not violate the Fourth Amendment and . . . does not deprive the government of the right to use evidence that it has acquired lawfully [from the private party].”).

¹⁷⁶ *Camara v. Municipal Court*, 387 U.S. 523 (1967) (holding that searches by regulatory officials conducting health and safety are subject to Fourth Amendment requirements).

¹⁷⁷ *Michigan v. Tyler*, 436 U.S. 499 (1978).

¹⁷⁸ *Marshall v. Barlow’s, Inc.* 436 U.S. 307 (1978).

¹⁷⁹ *Donovan v. Dewey*, 452 U.S. 594 (1981).

a government agency, that agency's actions would be governed by the Fourth Amendment constraints.

¶ 47 It is for this reason that trusted third party key escrow has been proposed both as a safeguard against potential government abuse and as an attempt to push back the point of government action to the time when law enforcement approaches the key escrow agent to obtain the key. The Justice Department has stated before Congress that obtaining the key by law enforcement in order to access the plaintext would constitute a search and would require a search warrant.¹⁸⁰ That said, it is critical to the feasibility of key escrow that the collection and escrow be structured in such a way that it will not constitute a government search. It is axiomatic that it would be impossible to meet the probable cause requirements to justify the collection of everyone's keys prior to any criminal conduct on their part if the Fourth Amendment applies to key escrow at the point of collection. Presumably, the vast majority of keys to be collected belong not to criminals but to innocent, law-abiding citizens for whom probable cause simply cannot be shown. In order for any potential key recovery to be held Constitutional under the Fourth Amendment, it must therefore either (a) not involve government action, or (b) not constitute a search.

¶ 48 The first logical step in trying to satisfy those requirements would be for someone other than the government to store the keys in a secure, recoverable fashion so that they can be obtained by law enforcement with a proper court order after a showing of probable cause and without the owner's knowledge or permission. Simply using trusted third parties does not, however, ensure that the collection of keys will not be construed as government action. Even for a strictly private citizen, courts examine the facts and circumstances surrounding the challenged conduct to determine if the party conducting the search or seizure was acting as an agent or instrument of the state.¹⁸¹ Courts have found sufficient state action where government agents actively participated in a search.¹⁸² Similarly, state action has been found where government officials instructed the private

¹⁸⁰ See Privacy in a Digital Age: Encryption and Mandatory Access: Hearings Before the Subcomm. on the Constitution, Federalism, and Property of the Senate Judiciary Comm., Mar. 17, 1998 (Prepared statement of Robert S. Litt, Principal Associate Deputy Attorney General) (visited Mar. 6, 1999) < <http://www.computerprivacy.com/archive/03171998-4.shtml> > .

¹⁸¹ See *Walter*, 447 U.S. at 656. See also *Coolidge*, 403 U.S. at 487 (“[T]he test . . . is whether [the private citizen], in light of all the circumstances of the case, must be regarded as having acted as an ‘instrument’ or agent of the state.”).

¹⁸² See, e.g., *State v. Cox*, 100 N.M. 667, 674 P.2d 1127 (App. 1983); *Corngold v. United States*, 367 F.2d 1 (9th Cir. 1966).

individual.¹⁸³ It would therefore seem that any mandatory rule of law that requires key escrow would be construed as government action whether the escrow agent was a government entity or a private party.

¶ 49

The government is therefore faced with a “Catch-22” situation in trying to structure its key recovery program. As key escrow becomes more absolute, and theoretically more effective at preventing illegal use of strong encryption by criminals and terrorists,¹⁸⁴ it looks more like government compulsion through the escrow agent and encryption companies, since there is no other means to legally obtain or export the encryption. In the absolute, the government is effectively forcing consumers to turn over their keys in order to get a product and companies to build in recovery mechanisms to be able to export their products, removing consumer choice altogether. While such government coercion maximizes the likelihood of preventing the illegal use of strong encryption, it also significantly increases the likelihood that the courts will construe the trusted third party to be acting as a government agent and bring the program one step closer to implicating the Fourth Amendment. Conversely, as key escrow becomes more of an incentive system for business to comply to gain the right to export or sell, less compulsion and possibly no compulsion may be imputed because the business, and not the government, is making the choice. It could likewise be argued that consumers still have a choice, namely to purchase and use strong, recoverable encryption or weak non-recoverable encryption.¹⁸⁵ At the opposite extreme, in which there is truly a choice, the trusted third parties are less likely to be considered government agents. If that is the case, then there is no government action and the Fourth Amendment is by definition not implicated.¹⁸⁶

¶ 50

It is equally true that even if the private party conducting the search is not considered a government agent, the government still cannot exceed the scope of

¹⁸³ See, e.g., *Skinner v. Railway Labor Executives Ass’n*, 489 U.S. 602 (1989) (holding that when alcohol and drug tests carried out by a private employer are mandated or strongly encouraged by government regulations, the Fourth Amendment applies).

¹⁸⁴ It should be noted that nothing in the Fourth Amendment analysis requires us to consider whether the key escrow plan will actually work to achieve its objectives. Only after a fairly technical analysis of whether there is government action, and whether the “government” conduct rises to the level of a search, do we even consider whether the search was reasonable.

¹⁸⁵ It is important to note that the courts have never found a privacy right to the use of encryption, much less non-recoverable encryption by individuals.

¹⁸⁶ The flaw in this argument, as will be discussed in Part V, *infra*, is that a partial or incomplete requirement for key recovery completely undermines the stated objective of preventing criminals and terrorists from obtaining strong, non-recoverable encryption products. If strong, non-recoverable encryption products exist in the marketplace, it is highly unlikely that the criminal element will opt for the recoverable version.

the prior non-government search without probable cause and a court order. The Supreme Court has generally refrained from regulating government searches that did not exceed the scope of the private search, but has held government conduct beyond the scope of the private search to Fourth Amendment standards.¹⁸⁷ This rule was explicitly interpreted to mean that a government search that is not a significant expansion of a search which had previously been conducted does not violate the Fourth Amendment.¹⁸⁸ Under *United States v. Jacobsen*, it is likely that the subsequent use of the escrowed encryption by law enforcement agencies will be considered to substantially exceed the scope of the third-party collection of those keys and will necessitate a search warrant.¹⁸⁹

¶ 51

Though the “private doorbell” system proposed by industry officials to satisfy export requirements is structured to require a warrant to gain access to the plaintext messages before encryption or after decryption, this actually constitutes less of a safeguard to privacy than key escrow. In the case of key escrow, law enforcement must obtain a Title III warrant to intercept electronic communications in real time or an ECPA warrant to access stored electronic communications. Under the Administration’s proposed key escrow program, if those messages turn out to be encrypted, the law enforcement agency must then show probable cause to believe that the message is encrypted using a particular individual’s key to obtain a second court order to compel the escrow agent to turn over the key in question. The “private doorbell” system removes that second layer of protection because it gives law enforcement, with a proper court order, direct access to the plaintext of the message.¹⁹⁰ It is also quite possible that the network operators who would have access to the plaintext of all of the messages and control their encryption would be able to read and willingly turn over messages implicating

¹⁸⁷ See *Walter*, 447 U.S. 649 (invalidating a conviction based on viewing of obscene films by the FBI, even though the private parties had opened the packages containing the films, and the film canisters indicated that they contained obscene films).

¹⁸⁸ See *United States v. Jacobsen*, 466 U.S. 109 (1984) (upholding the warrantless search of a damaged box previously opened and inspected by Federal Express employees).

¹⁸⁹ The Department of Justice has conceded that such use would require a warrant and has proposed additional authority, such as a court order or a separate warrant, beyond that required to intercept or access the encrypted message itself. See *Privacy in a Digital Age: Encryption and Mandatory Access: Hearings Before the Subcomm. on the Constitution, Federalism, and Property of the Senate Judiciary Comm.*, Mar. 17, 1998 (Prepared statement of Robert S. Litt, Principal Associate Deputy Attorney General) (visited Mar. 6, 1999) < <http://www.computerprivacy.com/archive/03171998-4.shtml> > .

¹⁹⁰ While this approach negates the need for a second court order, it should be noted that as the intercept is real time, the necessary court order is subject to the considerably more stringent requirements of Title III whereas the typical mode of gaining the encrypted messages under key escrow would be through an ECPA warrant to search stored electronic communications. As discussed in Part II, *supra*, the required showing to obtain a Title III warrant is considerably more rigorous than for an ECPA warrant.

criminal or terrorist activities to the government.¹⁹¹ If they did so, it is quite possible that the plaintext of those messages would be admissible, as the reading of the messages by law enforcement agents would not exceed the scope of the actions of the network operators under *Jacobsen*.

2. Key Recovery Without Search or Seizure?

¶ 52 A search is a government invasion of a person's reasonable expectation of privacy.¹⁹² Even if the key escrow or the private doorbell plan is found to constitute government action, the action will only be considered a search implicating the Fourth Amendment if an individual has an actual subjective expectation of privacy and society is prepared to recognize that expectation as objectively reasonable.¹⁹³ A seizure within the meaning of the Fourth Amendment will have occurred only when a governmental intrusion "meaningfully interferes" with an individual's possessory interest.¹⁹⁴

¶ 53 The commonly proposed structure for key escrow has been the secure storage of a copy of the encryption key by a trusted third party as a condition precedent to the sale or purchase of strong encryption products. The expectation is that once a message relevant as evidence in a criminal investigation is obtained by law enforcement agents, presumably after obtaining a proper warrant, the government will then request a separate court order to compel the trusted third party to release the escrowed key upon a showing of probable cause. It is useful for the

¹⁹¹ Undoubtedly, there are economic counterincentives such as loss of customers or fear of liability that would discourage the release of such messages to law enforcement without a court order. The point is merely that the Constitution does nothing to protect the privacy of the individual in the event that the network operator chooses to release the information despite the potential negative ramifications of such an action.

¹⁹² See *Oliver v. United States*, 466 U.S. 170, 177-78 (1984).

¹⁹³ See *Katz*, 389 U.S. at 361 (Harlan, J., concurring). At this point it is central to remember that the government has a powerful incentive to structure any key recovery or plaintext access scheme in such a way as to fall outside of the literal search definition as will be discussed in this section. If the program is considered a search, the collection of the keys must meet Fourth Amendment requirements of probable cause and a search warrant. This is not possible before the fact because the keys of the innocent as well as the guilty must be collected since the likelihood of their later criminal conduct that would require access to their plaintext messages cannot be determined in advance.

¹⁹⁴ Compare *Arizona v. Hicks*, 480 U.S. 321, 324-25 (1987) (finding no seizure when police recorded serial numbers of stereo equipment because no meaningful interference with defendant's possessory interest in either numbers recorded or stereo equipment; however, when police picked up stereo equipment, a search occurred because such action constituted new, unjustified invasion of privacy) with *Jacobsen*, 466 U.S. at 120 (seizure occurred when DEA agent asserted dominion and control over package at Federal Express Office).

sake of simplicity and clarity to consider the broadest possible key escrow program, one requiring escrow of all domestic as well as export encryption keys.¹⁹⁵

In such a broad key escrow program, there is unlikely to be a legitimate expectation of privacy in the encryption key. There can be no subjectively reasonable expectation of privacy if the key must be transferred to a third person in order to obtain the product.¹⁹⁶ There is also no objectively reasonable expectation of privacy if the regulatory scheme requires key escrow. The property interest and any expectation of privacy cannot attach until the key is obtained by the end user. If it is only legally possible to obtain a recoverable key, that expectation never attaches because the key is always subject to later seizure on a showing of probable cause and a court order. In a sense, the key owner has consented to the escrow of the key by buying the recoverable encryption product. In the proposed “all-encompassing”¹⁹⁷ key escrow scheme, concerns with government coercion of “consent” are most extant, but this does not affect the consideration of whether the conduct, which must already have been imputed to the government to reach this stage of the analysis, rises to the level of a search. Even in such a program, where the average American would only have access to recoverable encryption products, the alternatives, however inadequate, of using weak encryption or no encryption still provide some nominal measure of opportunity to “opt out” of the key escrow program.

¹⁹⁵ As discussed in Part III.A.1., *supra*, the broader the scope of key escrow, the more likely the courts will be to impute government action.

¹⁹⁶ Some concern has been expressed that an emphasis on the individual subjective expectation would allow the government to manipulate the Fourth Amendment, since it would depend on what people are used to, not what they should be entitled to expect. See *United States v. White*, 401 U.S. 745 (1971) (Harlan, J., dissenting).

Situations can be imagined, of course, in which Katz’ two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country, unaware of this Nation’s traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well. In such circumstances, where an individual’s subjective expectations had been “conditioned” by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a “legitimate expectation of privacy” existed in such cases, a normative inquiry would be proper.

Smith v. Maryland, 442 U.S. 735, 741 n. 5 (1979).

¹⁹⁷ As will be discussed in Part V, *infra*, it is a misnomer to consider any program implemented by the United States to be all-encompassing considering the development of encryption technology and products by other countries.

¶ 55 The degree of intrusiveness involved in the government action and the information obtained are also relevant considerations in determining whether a search has occurred.¹⁹⁸ The collection of the duplicate encryption key is likely to be considered a minimal degree of government intrusion on the individual's use of the key. The key holds no information itself,¹⁹⁹ only the means to translate lawfully acquired documents into readable plaintext. Under the posed plan, the Government does not even gain access to the key until probable cause is established and a warrant granted.

¶ 56 It is also likely that the presumptive collection of encryption keys will be considered a minimal, and not a meaningful, interference with the individual's possessory interest in the key. It will thus not constitute a seizure cognizable under the Fourth Amendment. If key escrow is secure, the key owner can still use the key safely.²⁰⁰ The individual possessory interest is defined at the point of purchase. If the government regulates so that only recoverable encryption is obtainable, then there will be no government interference. That is to say, if the regulation is structured so that it is, at least theoretically, impossible for individuals to ever obtain strong, non-recoverable encryption, then their possessory interest is by definition only the use of the strong encryption product subject to the limitation that the government may later be able to obtain the duplicate key and use it to read the plaintext of lawfully obtained messages encrypted with that duplicate key.

¶ 57 In short, the collection of encryption keys before any crime has been committed may not constitute a search or seizure subject to the Fourth Amendment. As is the case with the search of non-encrypted documents, the deterrent to misuse of encryption keys by the government once the keys are later obtained is already in place. The Fourth Amendment exclusionary rule would prohibit the admissibility of the underlying plaintext files acquired through an illegal search

¹⁹⁸ See *United States v. Place*, 462 U.S. 696, 707 (1983) (holding that the use of dogs to sniff for drugs does not constitute a search because the intrusiveness is minimal).

¹⁹⁹ The fact that the encryption key works to decrypt a potentially incriminating document may serve to identify the author or intended recipient of the message. See *infra* Part III.B.

²⁰⁰ This is a very controversial proposition that will be further investigated in Part V, *infra*. For the position of numerous industry and intelligence officials regarding the security of key escrow, see Hal Abelson et al, *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption* (June 8, 1998) < <http://www.cdt.org/crypto/risks98/>> (concluding that "[k]ey recovery systems are inherently less secure, more costly, and more difficult to use than similar systems without a recovery feature," and stating that the infrastructure required is beyond the competency of the field).

or seizure, just as it would in the absence of a key escrow program.²⁰¹ If the government were later to improperly acquire the keys from the trusted third party, this rule would also apply to bar the admissibility of the plaintext of files if the encryption key was obtained without a valid search warrant, regardless of whether the encrypted version of the document was obtained legally or not.²⁰² Key escrow does nothing to alter the legal standard for getting a search warrant for the underlying files; it only allows the police to read the plaintext once the files have been lawfully acquired. The Fourth Amendment, therefore, may not bar the implementation of even the sweeping key escrow program proposed above. As a result, it is not only possible but likely that a carefully structured key escrow program would drop out of the Fourth Amendment analysis at the threshold and that these important and laudable principles for protecting the privacy of Americans from government intrusion would never be brought to bear by the courts. The end result could be that the privacy of Americans would be compromised while criminals and terrorists simply went overseas to obtain strong, non-recoverable encryption to foil law enforcement scrutiny.

B. Mandatory Key Escrow May Not Implicate the Fifth Amendment

¶ 58

The Fifth Amendment “protects a person . . . against being incriminated by his own compelled, testimonial communications.”²⁰³ This protection extends to statements and acts, provided they are compelled, testimonial, and incriminate the person in a criminal proceeding. This protection applies not only to refusing to testify in criminal proceedings but also to the refusal “to answer official questions put to him in any other proceeding, civil or criminal, formal or informal, where the answers might incriminate him in future criminal proceedings.”²⁰⁴ “This privilege against self-incrimination helps prevent government from plundering the

²⁰¹ See *Weeks v. United States*, 232 U.S. 383, 398 (1914) (exclusionary rule applies in federal court to evidence obtained through Fourth Amendment violation), *overruled in part by Elkins v. U.S.*, 364 U.S. 206 (1960). The exclusionary rule also applies in state court to evidence obtained through a Fourth Amendment violation. *Mapp v. Ohio*, 367 U.S. 543, 654 (1961).

²⁰² See *Nardone v. United States*, 308 U.S. 338, 340-41 (1939) (conversations procured through an illegal wiretap inadmissible; evidence obtained as result of that information also inadmissible).

²⁰³ *Fisher v. United States*, 425 U.S. 391, 409 (1976). The Fifth Amendment provides that “no person . . . shall be compelled in any criminal case to be a witness against himself.” U.S. CONST. amend. V. The Fifth Amendment right against self-incrimination applies to the states through the Fourteenth Amendment. See *Malloy v. Hogan*, 378 U.S. 1, 8 (1964).

²⁰⁴ *Minnesota v. Murphy*, 465 U.S. 420, 426 (1984) (quoting *Lefkowitz v. Turley*, 441 U.S. 70, 77 (1973)).

defendant's own mind for assistance in convicting him of a crime"²⁰⁵ but like the Fourth Amendment, only provides protection if certain threshold criteria are met, namely that the communication in question be compelled by the government, testimonial, and incriminating.

1. *Compulsion*

¶ 59

The compulsion in question must be personal.²⁰⁶ A potential defendant cannot exert the Fifth Amendment privilege to prevent a third party in possession of documents owned by the defendant from producing those documents.²⁰⁷ Moreover, the Supreme Court has explicitly rejected a privacy basis for the Fifth Amendment.²⁰⁸ There is, furthermore, no protection for the contents of documents prepared voluntarily, since the element of coercion is absent.²⁰⁹ In the case of mandatory key escrow, the encryption key is a document with no incriminating information in it. Only the production of the key may be incriminating and the contents of the record are not protected in any case. The government has not required the defendant to create the key or to use it to encrypt potentially damaging documents. Since the individual has "voluntarily" entered the key escrow system, the contents of the encryption key are not protected because the key was voluntarily created for and used by the potential defendant to create the encrypted version of the message.²¹⁰ The escrowed encryption key is therefore a custodial

²⁰⁵ See Privacy in a Digital Age: Encryption and Mandatory Access: Hearings Before the Subcomm. on the Constitution, Federalism, and Property of the Senate Judiciary Comm., Mar. 17, 1998 (Prepared statement of Professor Kathleen M. Sullivan, Stanford Law School), on behalf of Americans for Computer Privacy) (visited Mar. 6, 1999) < <http://www.computerprivacy.com/archive/03171998-2.shtml> > .

²⁰⁶ See *Couch v. United States*, 409 U.S. 322, 328 (1973) ("The Constitution explicitly prohibits compelling an accused to bear witness 'against himself': it necessarily does not proscribe incriminating statements elicited from another. Compulsion upon the person asserting it is an important element of the privilege.").

²⁰⁷ See *id.* at 331 ("possession [not ownership] bears the closest relationship to the personal compulsion compelled by the Fifth Amendment"). The Fifth Amendment will not be discussed in reference to the industry-sponsored "private doorbell" program since it is the network personnel and not the potential defendant that produce the document, precluding any Fifth Amendment challenge by the defendant.

²⁰⁸ See *Fisher*, 425 U.S. at 401 ("We cannot cut the Fifth Amendment completely loose from the moorings of its language and make it serve as a general protector of privacy—a word not mentioned in the text and a concept directly addressed in the Fourth Amendment.").

²⁰⁹ See *United States v. Doe*, 465 U.S. 605, 610 (1984) (holding defendant's papers not protected when voluntarily prepared).

²¹⁰ *But see* discussion of compulsion in the context of imputed government action, *supra*, Part IV.A.1.

record that can be subpoenaed²¹¹ assuming that its production does not incriminate the custodian, in this case, the trusted third party.²¹² If an individual has entered the key escrow system knowing that at some future date, and on a showing of probable cause of his having committed a crime, law enforcement may be able to get a search warrant or wiretap authorization to get the documents as well as the key to read the plain text, his expectation of privacy is naturally somewhat reduced. In addition, Congress has already set a lower showing to gain access to electronic communications than to conduct a phone or wire tap.

2. *Incrimination*

¶ 60

The Fifth Amendment attaches only when a person's compelled testimony is incriminating.²¹³ The Supreme Court has held compelled testimony to be incriminating where reasonable cause exists to believe that a direct answer would support a criminal conviction or provide a link in the chain of evidence leading to such a conviction.²¹⁴ The answers must pose "substantial and 'real' and not merely trifling or imaginary hazards of incrimination."²¹⁵ Most importantly for the constitutionality of key escrow, the Fifth Amendment does not protect testimony or testimonial acts that may become incriminating through future conduct.²¹⁶ Since key escrow is predicated upon collection of strong encryption keys prior to any particularized showing or knowledge of particularized criminal activity, the key is not incriminating at the moment of collection. It is impossible for the end user to have used the key in some prior criminal activity that could make the production of the key itself incriminating, since he does not receive the software until after the duplicate encryption key is escrowed. As a result, struc-

²¹¹ See *SEC v. Jerry T. O'Brien*, 467 U.S. 735, 742 (1984) (finding no Fifth Amendment violation with respect to target of investigation when subpoena issued to third party because target not being compelled to produce materials).

²¹² Since the trusted third party is likely to be a corporate entity, the custodian will not be able to exert the Fifth Amendment privilege even in the unusual case where he might be personally incriminated by producing the key. See *Doe v. United States*, 487 U.S. 201 (1988) (holding that agents who accept custody of corporate or entity records do so in a representative capacity and assume the same obligation to permit inspection as the entity is lawfully required to assume).

²¹³ See *Estelle v. Smith*, 451 U.S. 454, 462 (1981).

²¹⁴ See *Hoffman v. United States*, 341 U.S. 479 (1951).

²¹⁵ *Marchetti v. United States*, 390 U.S. 39, 53 (1968) (reporting of illegal gambling income by frequent gambler reasonable basis for fear of incrimination).

²¹⁶ See *United States v. Freed*, 401 U.S. 601, 606 (1971) (holding National Firearms Act registration requirement did not violate the defendant's Fifth Amendment right even though disclosed information might be used in prosecution of future firearms offenses defendant could commit because no "substantial" or "real" hazard of incrimination).

turing a key escrow program so that the keys are collected by the manufacturer prior to sale precludes the quandary of trying to obtain the key from the potential defendant at some later point after he may have produced encrypted messages in a course of criminal conduct that could make the production of the key incriminating. When encrypted messages relevant to a criminal investigation are obtained by police, the police must then obtain a warrant before acquiring the key from the escrow custodian. In that case, the escrow custodian's act of production is not incriminating because the key owner does not produce the key.

¶ 61 This result, while apparently technically correct, is troublesome in that it appears that cleverly structuring the timing of collecting the keys to take the end-user out of the loop has effectively removed any Fifth Amendment protection. It can be argued that the structure is a product of the need to ensure that criminals and terrorists do not obtain strong encryption outside the system. Once a non-recoverable key is obtained, it is simply too easy to destroy an encryption key or claim the Fifth Amendment privilege and refuse to turn over the key to render the fruits of a lawful search useless. The merit of this argument turns on how different encryption is from previous technical advances. Is encryption such a technological marvel that law enforcement cannot possibly obtain the plain text messages necessary to successfully prosecute crimes in any other manner, so that the prior collection of the encryption keys of the innocent as well as the guilty is justifiable?²¹⁷ Conversely, it should be considered whether, if the prior key collection is permitted, adequate safeguards exist to protect the innocent users of strong encryption.

3. *Testimonial*

¶ 62 The Fifth Amendment is only implicated where a compelled communication is testimonial. "In order to be 'testimonial,' . . . [a communication] must itself, explicitly or implicitly, relate a factual assertion or disclose information" that expresses "the contents of an individual's mind."²¹⁸ While voluntarily prepared

²¹⁷ This argument is somewhat belied by the industry developed "private doorbell" system that gives law enforcement access to the plaintext of messages before they are encrypted at the point of origin or after they are decrypted at the destination. As stated previously, this may not completely undercut the argument for key escrow because it does nothing to prevent the end-user from "pre-encrypting" his message using strong non-recoverable encryption, if available, prior to sending the message across the network.

²¹⁸ *Doe v. United States*, 487 U.S. at 210 n.9, 215 (1988) (holding compelled signature of consent form authorizing foreign banks to release account information not testimonial because "neither the form, nor its execution, communicat[ed] any factual assertions, implicit or explicit, or convey[ed] any information to the Government").

papers are not shielded by the Fifth Amendment, the act of producing such documents is protected if the act itself is both testimonial and incriminating.²¹⁹ The act of production must reveal something other than a person's identity, appearance, or physical characteristics.²²⁰ The key itself is not evidence unless it creates a link for identity, authentication, or existence. However, if the verification provided by the act of production is unnecessary because the document's existence and accuracy are already independently verifiable, the act of production is not testimonial and thus is not covered by the Fifth Amendment.²²¹

¶ 63

Electronic communications will be gathered under a Title III warrant for real-time collection (not typically the case) or an ECPA warrant for collection from storage (more likely). Based on the context of how those files are acquired, the police will have to show probable cause to believe that the alleged criminal is the owner of the key that can decrypt the documents in order to obtain a court order to compel the trusted third party to release the key. The fact that the seized documents are encrypted informs law enforcement that a key to decrypt it must exist, or must have existed, or the messages would be useless to the intended recipient. The fact that probable cause must be shown to get the key means that law enforcement must have some form of other corroborating evidence to establish the identity of the key holder prior to obtaining the key. Therefore, the key only provides possible authenticating information. The fact that the key decrypts the message is evidence that the owner of the key encrypted it. In a public-key system, if someone's public key is used to encrypt a message, only that person's private key will decrypt it. This provides evidence that the message encrypted with the public key was intended for that individual. It is, however, the unprotected contents of the encryption key that permit the decryption of the underlying-

²¹⁹ See *United States v. Doe*, 465 U.S. at 612-14 (although the contents of sole proprietor's papers were not protected, producing papers was protected by Fifth Amendment because the act of production was testimonial and incriminated the holder of documents by admitting their existence and defendant's control over them, and tacitly admitting their authenticity).

²²⁰ The Court has upheld compelling a person to try on clothing to aid in identification, *Holt v. United States*, 218 U.S. 245, 252-53 (1910); to demonstrate speech or other characteristics, *Pennsylvania v. Muniz*, 496 U.S. 582, 592 (1990); to furnish hand writing samples, *United States v. Mara*, 410 U.S. 19 (1973); to submit to blood tests, *Schmerber v. California*, 384 U.S. 757 (1966); and to participate in a lineup, *United States v. Wade*, 388 U.S. 218, 223 (1967) (stating that the Fifth Amendment "offers no protection against compulsion to submit to fingerprinting, photography, or measurements, . . . to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture").

²²¹ See *Fisher*, 425 U.S. at 411 (Fifth Amendment privilege does not apply to compelled production of papers when existence and location forgone conclusions); *In re Grand Jury Subpoena Duces Tecum*, 1 F.3d 87,93 (2d Cir. 1993) (privilege does not apply to personal calendar when existence and location forgone conclusions and government could independently authenticate), *cert. denied*, 510 U.S. 1091 (1994); *United States v. Stone*, 976 F.2d 909, 911 (4th Cir. 1992) (*per curiam*) (privilege does not apply to defendant's personal records because existence not in dispute and records could be authenticated by other means).

ing message and thereby provide the identifying evidence that the key owner either encrypted the message or was the likely recipient.

¶ 64

It should also be noted that since the encryption key is duplicated prior to the end-user taking custody of the software, it is technically not the end user who is surrendering the key. Therefore, he can neither be considered to be under compulsion or to be committing a testimonial act. Only when used to encrypt a plaintext document will access to the encryption key potentially become of interest to law enforcement officials. To obtain the key from the trusted third party, the police will, by definition, have to know to whom the key belongs. However, it is only after some encrypted electronic document is obtained through other legal means, and with probable cause to believe it was encrypted by or for a particular individual, that the police will be able to make the required showing to obtain a court order for the release of the key. The fact that the future defendant turns over the key makes a statement that “this is my key.” The fact that the self-identified key is later associated with an incriminating document may prove incriminating to the individual, but the Fifth Amendment does not protect testimonial acts that may be made incriminating by later conduct.²²² Even if the act of production is protected by Fifth Amendment, the underlying document, i.e., the key, is not protected.

¶ 65

Additionally, a defendant is precluded from claiming a Fifth Amendment privilege to refuse production of documents if the government grants immunity for the testimonial acts of production.²²³ Making the act of producing the key itself inadmissible by granting statutory use immunity may resolve this problem and strike a better balance between privacy and security.²²⁴ The act of production is of little importance to the prosecutor’s case, since it is the underlying message that is the primary evidence of criminal wrongdoing. The authentication of the source or recipient of the message must be independently justified before a court order for access to a particular escrowed encryption key can issue. In short, law enforcement gains little from attempting to admit the act of production. Providing statutory immunity for that act effectively immunizes key escrow from Fifth Amendment challenge.

²²² See *Freed*, 401 U.S. at 606.

²²³ *United States v. J.W.O.*, 940 F.2d 1165, 1167 (8th Cir. 1991).

²²⁴ The grant of immunity need only be congruent with the privilege, which only prevents compelled incrimination. See, e.g., *Ullmann v. United States*, 350 U.S. 422 (1956). See Philip R. Reiting, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171 (arguing that encryption keys or the plaintext of messages should be able to be subpoenaed if the act of production is immunized).

¶ 66 In short, there is a real danger that courts may interpret a carefully structured key escrow program not to implicate the Fourth and Fifth Amendments. The end result could be that the privacy of Americans would be compromised, while criminals and terrorists simply went overseas to obtain strong non-recoverable encryption to foil law enforcement scrutiny.

V. IS KEY RECOVERY PRACTICAL?

¶ 67 Having concluded that the Constitution and existing law do not effectively bar the development of a mandatory key escrow system, I will now turn to what should be the most fundamental questions: will key escrow work, and is it justified? That is to say, will key escrow as proposed effectively bar the use of strong encryption by criminals and terrorists to further their criminal enterprises? While this seems an eminently logical question to ask, we must consider what is required to stop criminal and terrorist use of encryption and whether it can be achieved. Only after these questions have been answered do we reach the critical question: is accomplishing the admittedly laudable objective of barring the use of encryption by criminals and terrorists for illegal activity worth the sacrifice in privacy? I will now turn to consideration of whether the proposed key escrow plan will meet the stated objectives, what the consequences are of meeting those objectives, and, finally, whether the result is worth the consequences.

A. *Will It Work?*

¶ 68 Is it possible to create a key escrow system that will achieve law enforcement and national security objectives of keeping strong, non-recoverable encryption out of the hands of criminals and terrorists? Presumably, a system wherein all strong encryption products, worldwide, are escrowed with absolutely no leakage would be the ideal system from a purely objective standpoint. While such a system would have the greatest likelihood of success, it would require that all encryption-producing nations imposed the same escrow requirement. In the absence of an international consensus, the U.S. would be left with a system wherein all U.S. products were escrowed, both domestically and for export, while strong non-recoverable products were freely available overseas. Even if the U.S. were the only encryption producer, which it is not, the free availability of strong, non-recoverable encryption products in this country has the potential to undermine the export controls so elaborately developed to safeguard the release of U.S. encryption to other countries. With essentially unregulated access to the Internet,

products freely available in the U.S. find their way to foreign websites.²²⁵ In such a system, a criminal or terrorist would merely have to go overseas to get strong encryption products that would be unbreakable by U.S. law enforcement.²²⁶ While there has recently been some agreement about the need to create an international key escrow system, such a system is far from absolute and the U.S. has limited ability to control the proliferation of strong, non-recoverable encryption software beyond its borders. That said, even if the U.S. key escrow system were absolute, there would be significant concerns over its effectiveness in controlling access to strong encryption by criminals and terrorists. In reality, the system in the U.S. has been one of free access to strong encryption of any length, whether recoverable or not. It is this very leaky sieve that has prompted FBI director Louis Freeh to argue so forcefully for domestic key escrow.

¶ 69

Putting aside, for the moment, the political and Constitutional concerns that would be raised by such a system, it could be argued that such a system is already doomed to failure. Free access in this country to strong, non-recoverable encryption has made it widely available to criminal and law abider alike. It seems unlikely that if a law were passed to implement a widespread key escrow system, criminals would come forward and turn in their keys. Even if criminal penalties were instituted for the possession of strong non-recoverable encryption, it is unclear whether those already engaged in criminally punishable activities would be significantly deterred. Quite possibly the effect of such an ordinance would be that law abiding citizens would turn in their keys while criminals continued to foil law enforcement efforts to monitor their communications by continuing to use encryption products already freely available today.²²⁷ Compounding this problem would be the fact that any federal legislation would likely set some future date to commence key escrow, allowing criminals to obtain the strongest currently available encryption and permitting them to send unbreakable messages for years to come. It should also be noted that there is considerable political

²²⁵ For example, version 2.6 of PGP, a popular military-grade cryptography program, appeared on a German website within days after being released as freeware in the United States by graduate students at MIT. The program was sent to Hamburg via an anonymous remailer. See Froomkin, *supra* note 75, at 750 (1995).

²²⁶ In fact, the Department of Justice recognizes that commonly available encryption products are already so strong that U.S. law enforcement agencies cannot break them. See *Privacy in a Digital Age: Encryption and Mandatory Access: Hearings Before the Subcomm. on the Constitution, Federalism, and Property of the Senate Judiciary Comm.*, Mar. 17, 1998 (Prepared statement of Robert S. Litt, Principal Associate Deputy Attorney General) (visited Mar. 6, 1999) < <http://www.computerprivacy.com/archive/03171998-4.shtml> > .

²²⁷ The author was able to purchase a 160-bit general-purpose symmetric-key encryption product for \$9.99 at the local Fry's Electronics store.

support for continuing the free access to strong non-recoverable encryption in the U.S. It is therefore unlikely that an absolute, prospective escrow program would be passed by Congress, much less a program that required individuals to retroactively turn in their keys. As a result, the realization that any key escrow program from this point forward will be but a partial solution is perhaps most critical to the entire practicality discussion. Regardless of what program is implemented going forward, the best law enforcement can hope for is to collect some, but not all, of the keys, and effectively to stop the proliferation and ostensibly to prevent an exacerbation of the situation. In addition, the Administration's recent move to exempt large industry sectors from export controls and to allow them to export products of any length, whether recoverable or not, will provide a potential source for criminals and terrorists overseas to obtain the very products that U.S. law enforcement hopes to keep out of their hands.²²⁸ Considering the preceding factors, it seems clear that keeping strong, non-recoverable encryption completely out of the hands of criminals and terrorists is not practical in the near term. If absolute victory for law enforcement is not achievable, it then becomes a matter of weighing the benefit to law enforcement of a partial key escrow system against the cost to industry and the American people. That is not to say that law enforcement concerns regarding the widespread use of non-recoverable encryption are not legitimate, but rather that, considering the current state of affairs and the relatively free availability of strong, non-recoverable encryption products on the world market, it is irrational and unjustified to try to place artificial restrictions on products for U.S. and export markets that are already freely available worldwide. These sorts of restrictions are not going to affect the criminal element that is being used to justify their imposition. Rather, lawful users and the United States encryption industry will suffer while the criminals simply look elsewhere.

B. What Are the Consequences of Trying to Make It Work?

¶ 70

It is not just criminals and terrorists who would be affected by widespread adoption of key escrow. The administration's efforts to date have already had a lasting effect on the balance of power in the worldwide encryption industry to the detriment of American companies. In addition, mandatory key escrow poses

²²⁸ See *Implementing New Financial Encryption Policy: Interim Rule Not Just For Banks*, EXPORT PRAC., Oct. 15, 1998, at 11 ("Of course, the question yet to be determined is: Is there any realistic hope of controlling strong encryption product exports and availability to dangerous end-users once exports are permitted to all the sectors targeted for 'updating'?").

significant security and privacy concerns that must be considered in weighing the merits of any potential key escrow program.

¶ 71

As early as 1996, there were indications that the U.S. encryption industry was suffering from the Administration's strict export controls and "carrot and stick" approach to encouraging key escrow. A government study ordered by Vice President Gore and National Security Advisor Anthony Lake found that existing U.S. restrictions on exports of software with encryption capabilities have hampered the ability of U.S. exporters to compete in world markets. The study, done by the U.S. Commerce Department and the National Security Agency, also found that the growth of the global market for such products has been slowed by strong export controls, both in the United States and other countries.²²⁹ U.S. export controls have additionally led to the belief in many countries that exportable U.S. encryption products are of "unsatisfactory quality."²³⁰ While U.S. companies had difficulty quantifying the economic impact of export controls, they were able to provide substantive examples of how they had been adversely affected. Some companies had curtailed their plans to expand security features to meet anticipated growing demand as a result of export controls. Others cited "administrative burdens" and "time delays" as deterrents to applying for licenses, with some larger companies either developing two versions of software or incorporating an encryption algorithm that they knew would qualify for Commerce general licenses. "Many smaller, security-specific software firms said that they have elected to limit their sales to the U.S. market, and that they have lost potential sales overseas, where the market is believed to be sizable."²³¹ The final conclusion of the study was that "the competitive advantage that foreign companies derive from their ability to meet the growing demand for cryptographic products may result in lost market share for U.S. companies. It said that, over time, the U.S. government's restrictive practice threatens to drive sales, technologies, and jobs to foreign

²²⁹ See Yerkey, *supra* note 91, at 85.

Of the 31 countries surveyed, sources in 14 countries reported that U.S. export controls were limiting U.S. market shares in their countries, while sources in most countries indicated that U.S. market share was keeping pace with overall demand despite the impact of U.S. controls Three major exceptions were noted: Switzerland, Denmark, and the United Kingdom, where sources attributed a decline in U.S. market share to U.S. exports controls, which, according to the unnamed sources, promote the development and sale of indigenous encryption products.

Id.

²³⁰ See *id.*

²³¹ *Id.*

competitors able to export such products.”²³² Another phenomenon that can be attributed to export controls is the “export” of encryption production offshore in an effort to legally bypass the export controls.²³³

U.S. export controls applied to encryption technology have already had unintended commercial consequences. U.S. developers of encryption software have, for example, moved aggressively to create foreign ventures and to develop sophisticated encryption software through those ventures. The products developed abroad can be freely exported, not subject to U.S. export controls.²³⁴

¶ 72

Perhaps the largest single beneficiary of U.S. export regulation has been the European encryption industry.²³⁵ Numerous European companies have been forced to turn to smaller European companies that “don’t face any restrictions, rather than buy the watered-down software the U.S. allows for export.”²³⁶ The export controls have also forced U.S. companies to turn away new business when it turns out the potential customers are located overseas.²³⁷

²³² *Id.* at 86.

²³³ See Dan Goodin, *True Tales from the Encrypt*, LEGAL TIMES, Apr. 21, 1997, at 2 (“This is not a case of people flouting the law.’ . . . The companies ‘have come up with real gaps in the coverage of the export control laws and have some reason to think what they’re doing can be done,’ said [Stewart] Baker [former NSA general counsel]”).

²³⁴ Jeffrey H. Matsuura & George B. Delta, *Export Controls on the Internet*, 10 J. PROPRIETARY RTS. 2, 11 (Mar. 1998). RSA Data Security, Inc. is developing software in Japan and Sun Microsystems in Russia, numerous smaller developers, such as C2Net Software, Inc., are taking a similar approach. *Id.* (“To the extent that U.S. regulations remain rigorous, more U.S. software developers are likely to follow this process. While U.S. software developers are actively expanding their foreign development efforts for many economic and technical reasons, at least some of those companies are moving abroad to find relief from U.S. export restrictions.”).

These cooperative arrangements allow U.S. companies to provide complete security solutions by encouraging their foreign partners to marry foreign-made crypto with U.S. commercial applications. These cooperative arrangements are highly risky under U.S. law, but they are not unlawful per se. Given the stakes, many companies have been prepared to take risks under U.S. law, and it is expected that more will do the same. *Findings of the President’s Export Council Subcommittee on Encryption* (Sept. 18, 1998) < <http://209.122.145.150/PresidentsExportCouncil/PECSENC/pecsenc1.htm> > .

²³⁵ See Kimberley A. Strassel, *U.S. Rules Boost Europe’s Encryption: European Competitors Cash In on U.S. Export Limits*, WALL ST. J., July 7, 1998, at B6. Europe has not, however, been the only beneficiary. Findings of the President’s Export Council Subcommittee on Encryption, *supra* note 234 (noting that U.S. encryption policy has fostered the development of cryptographic software and hardware skills outside the United States and that German, Swiss, Canadian, Russian, and Israeli cryptography companies have all benefited).

²³⁶ “It would have been like importing a tank without a cannon,” says Michael Schmidt, an Internet consultant for Allianz, a German company who selected a German encryption start-up for encryption software for its Internet site. “We couldn’t risk it. We had to use a European company.” Strassel, *supra* note 235 at B6.

²³⁷ RSA Data Security Inc., a leading U.S. encryption-software firm reports turning away overseas giants that called looking for deals: Lloyds TSB PLC, SAP AG, Siemens AG, and Cie. des Machines Bull, to name a few. Meanwhile, Microsoft Corp. reports losing “hundreds of thousands” of potential users of its software. Consensus Development Corp., which licenses encryption to firms such as International

¶ 73 While differences between U.S. and foreign encryption controls are a major hindrance to the overseas sale of U.S. encryption products and other software that relies on them, the success of U.S. companies in the market is also hindered by foreign government influence in software purchases, inherent biases in favor of local producers, and reluctance to “deploy serious security technology until there have been major incidents with losses that can be attributed to lack of encryption.”²³⁸ “[O]ne particularly serious risk is that non-U.S. companies will use their ability to export stronger encryption as ‘leverage’ to dominate particular applications.”²³⁹ According to the President’s Export Council Subcommittee on Encryption (PECSENC), “[l]oss of U.S. competitiveness in the electronic commerce software market obviously raises concerns not just about encryption software but other software opportunities. Indeed, it foreshadows a weakening of the U.S. position as a leader in electronic commerce generally.”²⁴⁰

¶ 74 In addition to its significant economic impact on the U.S. encryption industry, the key escrow program sought by the Clinton Administration adds a new degree of complexity and an additional layer of risk exposure that are not present in the use of non-recoverable encryption products.

¶ 75 In 1997, a group of eleven prominent cryptographers analyzed the technical challenges and potential costs of a key recovery system that could meet the Administration’s stated requirements. The end result of that study was a report highly critical of both the economic feasibility and the privacy and security consequences of meeting law enforcement objectives.²⁴¹

All key-recovery systems require the existence of a highly sensitive and highly-available secret key or collection of keys that must be maintained

Business Machines Corp., says it loses about 40% of new-business leads because they turn out to be overseas clients. *Id.*

²³⁸ Findings of the President’s Export Council Subcommittee on Encryption, *supra* note 234.

²³⁹ *Id.*

This has happened in at least one field—Internet banking—and may occur in other areas of electronic commerce. Brokat, a German company that scarcely existed four years ago, now has 250 employees and offices in several countries including the United States. Brokat’s specialty is Internet banking and electronic commerce, but it broke into that business on the strength of being able to offer stronger encryption than German banks could obtain in Netscape or Microsoft browsers. It is now a major player in this niche, with 50% of the European Internet banking market and enough U.S. customers to justify a 20-person U.S. branch office. Meanwhile, encryption constitutes 10% or less of Brokat’s revenue, and it has expanded its initial Internet banking offerings to include support for other forms of electronic commerce.

Id.

²⁴⁰ *Id.*

²⁴¹ *Id.*

in a secure manner over an extended time period. These systems must make decryption information quickly accessible to law enforcement agencies without notice to the key owners. These basic requirements make the problem of general key recovery difficult and expensive—and potentially too insecure and too costly for many applications and many users.²⁴²

Most significantly, the study concluded that “[t]he deployment of key-recovery-based encryption infrastructures to meet law enforcement’s stated specifications will result in substantial sacrifices in security and greatly increased costs to the end-user.”²⁴³ While recognizing the potential utility of key escrow to certain end users and applications, the report stressed that the needs of government are very different from those of other users and ultimately impose “substantial new risks and costs.”²⁴⁴ The requirements put forward to meet law enforcement demands for such global key recovery systems include (1) “[t]hird-party/government access without notice to or consent of the user,” (2) “[u]biquitous international adoption of key recovery,” (3) “[h]igh-availability, around-the-clock access to plaintext under a variety of operational conditions,” and (4) “[a]ccess to encrypted communications traffic as well as to encrypted stored data.”²⁴⁵ As discussed in Part III.B.2, *supra*, the more ubiquitous the key recovery system, internationally as well as domestically, the greater the likelihood that law enforcement objectives will be accomplished. In contrast, the limited market sectors that stand to benefit from key escrow do not require the participation of all encryption users to gain that benefit. Additionally, industry users of key escrow are highly unlikely to require response times on the order of hours that are being demanded by law enforcement. Similarly, there is little if any private demand for real-time interception of electronic communications, one of law enforcement’s central requirements. This is particularly significant considering the substantially different requirements under Title III and the ECPA for real-time interception compared to access to stored communications.²⁴⁶

¶ 76

The difficulty with imposing these non-market-driven requirements on all users is that it will expose many users who have little need or potential for per-

²⁴² Hal Abelson et al., *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption* (visited June 3, 1999) < <http://www.cdt.org/crypto/risks98/> > .

²⁴³ *Id.*

²⁴⁴ *Id.*

²⁴⁵ *Id.*

²⁴⁶ See *supra* Part II.

sonal “benefit” from key escrow to enhanced risk and reduced privacy. Key escrow takes the absolute control for access to plaintext out of the hands of the user. By its nature, it creates an alternate path to the plaintext of messages intended to be private and secure. In answer to law enforcement requirements for rapid access, this path must be readily accessible, further limiting the opportunity to safeguard the plaintext of the message. Key escrow is intended to act as a system in which third parties are trusted with the control of this alternate path to plaintext and are expected, even legally bound, to render assistance in utilizing the alternate path without the knowledge or consent of the key owner. This inherently introduces the potential for abuse, either by law enforcement or the trusted third party. Much of the legislation proposed to date has included some degree of protection against improper release of information and has included procedural safeguards to prevent improper access to plaintext messages by overzealous law enforcement agents. Indeed, the Fourth Amendment, Title III, and the ECPA already provide a patchwork of protection for electronic communications; one, however, that arguably underprotects the privacy and security of electronic communications. The very existence of concentrated key escrow agents, with their necessary repository of secret keys, creates a very high-value target for criminal attack. The possibility exists that the theft of a single private key or a small number of keys could unlock significant portions of an individual’s or a company’s data. The added element of secrecy required to provide surreptitious law enforcement access without user notice or knowledge greatly increases the risk by moving the point of escrow further away from the end user. While many end user requirements for key recovery could be handled locally and with the knowledge of the key owner,²⁴⁷ the law enforcement need for recovery

²⁴⁷ See Abelson, *supra* note 200:

For a key recovery scheme to be of value to the encryption user, it must allow tight control over depositing, recovering, and maintaining keys, tied to the user’s own practices and requirements. Generally, only a small number of individuals will need the ability to recover any individual key, often working in the same location and personally known to one another. When a key does need to be recovered, it will frequently be a local matter, similar to the replacement of a misplaced office key or restoring a computer file with a backup copy. . . . Similarly, there is usually no business need for secrecy in the recovery of keys or for the ability to obtain keys without the initial cooperation of the user. [When] key recovery is used in a business environment, it would generally be one component of the overall data management policy of that business. Users would normally be trusted to participate in assuring recoverability of their own keys, assisted by local management practices and supervision. When a key must be recovered, it will usually be because the users themselves realize that they do not have a copy of the correct key or because the key-holder is no longer available. Even the frequently-cited hypothetical example of the disgruntled employee who refuses to decrypt important files is probably most reliably and economically dealt with through business data management practices (such as management supervision and backup of business-critical plaintext) that do not require any central-

without the user's knowledge requires use of a trusted third party who is removed from the user. While these measures may seem eminently logical from the perspective of law enforcement, the fact that individual users have very different motives and purposes for using encryption create inherent difficulties for applying any "one-size-fits-all" key recovery program.

¶ 77

There should be some substantial fit between the government's goals and the measures it uses to achieve those goals. Few would dispute that criminal and terrorist use of strong encryption to elude law enforcement is detrimental to public safety and national security. It does not necessarily follow that any regulation that has the slightest opportunity of blocking criminal access to strong encryption should therefore be embraced. Personal privacy, highly prized by the American people, must weigh into the calculation, as must the concrete economic harm to U.S. business competitiveness overseas.

VI. CONCLUSION: WHAT SHOULD CONGRESS DO?

¶ 78

Even though it may be possible to draft key recovery legislation that passes Fourth and Fifth Amendment muster, the use of piecemeal key recovery that exempts entire industries (i.e. financial institutions, insurance companies, and online merchants) provides so many opportunities for the criminal element to obtain strong non-recoverable encryption that such legislation would be reduced to a futile gesture and a needless infringement on the privacy of average citizens. While a partial key recovery system may avoid some of the Constitutional concerns, it will not only fail to stop criminals and terrorists from using encryption to further their crimes, but also create a potential Achilles' heel that may stunt the growth of electronic commerce and facilitate cybercrime. Even if there is a compelling law enforcement interest in key recovery, the current proposal fails to satisfy that interest, while lessening personal privacy. The only way to completely stop criminals and terrorists from using strong encryption for illegal purposes is to make sure every piece of encryption has key recovery built into it. Once strong non-recoverable encryption has been disseminated (which it already has), there is no way to reliably contain it. The U.S. is a single player in a global marketplace and has had limited success in generating international support for key recovery. The current system has far too many holes to be effective against enterprising criminals and terrorists. Key recovery does not appear to be consti-

ized, standard key recovery mechanism. Even in this (rather unusual) case, there is no need to hide from the user the fact that a key has been recovered.

tutionally barred, but it is so ineffective in its current form as to undercut the policy justifications for its existence.

¶ 79 The newly proposed “private doorbell” system only begins to answer the problems of key recovery. Constitutionally, it is less assailable because it does not compel individuals to release their keys, thus avoiding possible Fifth Amendment scrutiny. The structure of the network and the timing of encryption and decryption preserve future access by law enforcement to the plaintext of messages, but they also introduce a weakness that can be exploited by the very criminal element they are intended to foil. The “private doorbell” system also does nothing to prevent or respond to the very real possibility that the end user will encrypt the message using strong, non-recoverable encryption before ever sending it across the network. In short, like key escrow, the “private doorbell” system creates a weakness in the armor of strong encryption without achieving the stated goals of barring criminals and terrorists from using strong encryption to further their illegal operations.

¶ 80 The threat that the courts will place a carefully structured key escrow program outside the ambit of the Fourth and Fifth Amendments is too great to be allowed to run its course. Considering the motivations behind the Fourth and Fifth Amendments and the fact that the legal precedent has evolved to create a flaw or back door in the protection of privacy, it is essential that Congress act to protect the individual privacy interests at stake, because the courts likely will not. The courts have historically had difficulty applying the strictures of the Fourth and Fifth amendments to new and emerging technology and have had a tendency to apply existing legal tests created at a time when the new technology was inconceivable. On prior occasions, the result has sometimes been to underprotect individual privacy interests and to necessitate congressional action to provide adequate protection.

¶ 81 The threat of nationwide or worldwide key escrow provides another such opportunity for Congress to correct the time lag in the judicial response to the advance of encryption. The result of the congressional gridlock has been free rein for the Administration to over-regulate encryption exports and to underprotect individual privacy and U.S. commercial interests. Just as Congress enacted Title III to deal with advances in eavesdropping technology and the ECPA to respond to the widespread use of computers for interpersonal communication, the time is ripe for Congress to respond to technical advances in encryption that form the cornerstone of future advances in electronic commerce. Congress should therefore pass legislation in the spirit of the SAFE bill reintroduced in the 106th Con-

gress to ensure free access to strong, non-recoverable encryption in the United States and to restore the competitiveness of the U.S. encryption industry. This would be accomplished by including provisions permitting the free export of encryption of any length, with or without key escrow, so long as comparable products are freely available on the world market and barring mandatory key escrow. By taking decisive action, Congress can seize the opportunity to protect the development of electronic commerce and the free development of the Internet in general, while, most importantly, providing adequate protection for individual privacy interests. While the Administration's stated objectives of protecting law enforcement and national security interests in the access to the plaintext of encrypted messages are respectable, the course on which the Administration has embarked to achieve those objectives is ill-conceived and doomed to failure, considering the state of proliferation of non-recoverable encryption in the world today. These policies have had a disparate impact on individual privacy and the commercial competitiveness of U.S. encryption firms while not significantly advancing the interests of law enforcement and national security. The interests at stake, both individual privacy and U.S. commercial competitiveness, are too considerable to leave to the vagaries of the courts' analysis and potential under-protection under the Fourth and Fifth Amendments.