University of Chicago Legal Forum

Volume 1996 Article 3

1996

It Came from Planet Clipper: The Battle Over Cryptographic Key "Escrow"

A. Michael Froomkin

Follow this and additional works at: http://chicagounbound.uchicago.edu/uclf

Recommended Citation

Froomkin, A. Michael (1996) "It Came from Planet Clipper: The Battle Over Cryptographic Key "Escrow"," *University of Chicago Legal Forum*: Vol. 1996, Article 3.
Available at: http://chicagounbound.uchicago.edu/uclf/vol1996/iss1/3

This Article is brought to you for free and open access by Chicago Unbound. It has been accepted for inclusion in University of Chicago Legal Forum by an authorized administrator of Chicago Unbound. For more information, please contact unbound@law.uchicago.edu.

It Came From Planet Clipper: The Battle Over Cryptographic Key "Escrow"

A. Michael Froomkin†

The emergence of cryptography as an integral part of modern communications and data storage creates dilemmas for government policy makers. The national interest is clearly well served when citizens have access to secure telecommunications and data storage.[1] The increased use of computers and computer-aided communications such as local area networks ("LANs") and the Internet means that digitized data plays an increasing role in modern life. This digitized data—which can be anything from business's most valuable trade secrets to copyrighted music to intensely personal information—is particularly vulnerable data: it is easy to copy, and often relatively easy to access also. Routine use of encryption means that businesses are better protected against industrial espionage by competitors and foreign governments.[2] It reduces information theft and attacks by "hackers" or

---

† © A. Michael Froomkin, 1997. All rights reserved. Associate Professor, University of Miami School of Law. Internet: froomkin@law.miami.edu. Caroline Bradley, Carl Ellison, Tim Philp, Mark Rotenberg, and Willis Ware made helpful comments at the outline stage; Dorothy Denning and Carl Ellison provided helpful technical information; Brooks Fudenburg, Patrick Gudridge, and Adam Smith made helpful comments on an earlier draft; none should be assumed to necessarily agree with my analysis or conclusions. Thank you to SueAnn Campbell and Nora de la Garza for library support and to Rosalia Lliraldi for secretarial assistance.

I am grateful to Larry Lessig and the *University of Chicago Legal Forum* for inviting me to participate in the Law of Cyberspace symposium. I particularly want to acknowledge the editors of the *Legal Forum* for tolerating my desire to present an up-to-date account of a rapidly changing subject. Thus, although a preliminary draft was delivered in Chicago on November 4, 1995, unless otherwise noted this Article attempts to reflect legal, political, and technical developments as of July 15, 1996.

At the request of the National Research Council I reviewed an early draft of its report on cryptography policy, which is discussed in this article, and submitted comments to the Committee.

[1] See National Research Council, Kenneth Dam and Herb Lin, eds, *Cryptography's Role in Securing the Information Society* 22-50 (National Academy Press, 1996) ("*CRISIS Report*"). The National Research Council is part of the National Academy of Sciences.

[2] National Counterintelligence Center, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* 15 (1996). According to FBI Director Louis Freeh, the governments of at least 20 nations are "actively engaged in economic espionage." Louis J. Freeh, *Address at the Executives' Club of Chicago* 8 (Feb 17, 1994) (tran-

saboteurs who could theoretically disrupt banking and finance, utilities including telecommunications and the power grid, and even components of the national defense.[3] Encryption also enhances the ability of citizens to protect their privacy against intrusions ranging from illegal government investigations to nosy relatives.

The greatest dilemma arises from the fact that techniques that protect against illicit eavesdropping and data theft also threaten to prevent *licit* access to communications and data by law enforcement and intelligence agencies.[4] The policy dilemma is especially acute in the United States because widespread encryption imposes a particularly severe cost on U.S. intelligence-gathering capabilities. (I use "capability" throughout this Article to mean *physical* ability, not legal ability. Thus, for example, anyone with a gun who can get within range has the capability of shooting me. That doesn't mean they legally can, morally should, or likely will.) U.S. electronic-intelligence capabilities are presumed to be the best in the world; if so, the U.S. has the most to lose from a move towards a world in which communications traffic is routinely protected with encryption so strong that it cannot be decrypted easily, and perhaps not at all. Widespread high-quality encryption not only lessens the U.S. government's ability to eavesdrop on foreign communications, but threatens to make it difficult, perhaps impossible, to conduct traffic analysis. Where once an encrypted message stood out, suggesting that the sender had something important to hide, now these critical messages risk being camouflaged in a sea of encrypted data.

Encryption policy also involves a subtle interrelationship between domestic and foreign policy. Although there are no legal controls on the production or use of strong cryptographic products by U.S. citizens or residents within the U.S., these products

---

script available at the FBI) (excerpts available online at http://www.hotwired.com/clipper/fbi.quotes.html).

[3] See *CRISIS Report* at 2 (cited in note 1); U.S. General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, GAO/AIMD-96-84 (May 1996).

[4] Not everyone accepts that the government should have the right to acquire the contents of personal communications and data. Nevertheless, in this article I will assume without argument that surveillance and information acquisition conducted pursuant to the rule of law, such as a valid warrant or other lawful government order, is the legitimate fruit of a legitimate policy choice in a democratic society. From this perspective—which is surely the perspective of policy makers who have the duty of executing those laws—legitimate national policy is frustrated when a wiretap is thwarted because the FBI cannot decode the conversation or a search warrant is unproductive because the police cannot decrypt the suspect's hard drive.

cannot be exported or sold to foreigners. Export control likely retards the spread of cryptography in the U.S.[5] Conversely, efforts to preserve the domestic wiretapping and data-search capabilities of law enforcement by technical means such as the Clipper chip would risk hampering the sales of U.S. products if comparable local products that are not wiretap-ready are available abroad.

At its deepest level, the encryption dilemma implicates profound questions about the relationships among citizens, and between the citizen and the state. The fundamental issues revolve around trust: whether citizens should be asked to trust the state with the means of acquiring the citizens' secrets, and whether the community and the state[6] feel they can afford to allow citizens, as well as foreign citizens and foreign states, access to technologies that enhance secret-keeping to the point that police or intelligence agencies might find it impossible to monitor communications or search a computer's hard drive.

This Introduction will briefly sketch the export-control regime as it applies to cryptography, and discuss the evolving goals of U.S. cryptography policy. The three main sections of this paper are each devoted to a phase of the U.S. government's recent attempts to keep the cryptography genie in the bottle in the face of increasing commercial and political pressure to loosen or abolish cryptographic export control. Part I offers a quick summary of the late, unlamented Clipper chip initiative.[7] Part II describes the Clinton Administration's proposal for software-based key "escrow." Part III, the longest part, begins in section A by discussing recent technical and political changes that make the current export control policy increasingly difficult to maintain. Section B examines the Administration's cryptographic "*White Paper*" which proposes legislation to require that the national information infrastructure be designed to ensure that any communication, and any transaction, that it facilitates is exposed to possible government monitoring. Section C briefly surveys international initiatives, at least welcomed and perhaps

---

[5] See Part I.B.

[6] Whether "the state" can usefully be personified, and once so reified can usefully be said to have interests of its own separate from and perhaps even inimical to the community, are problems I must gloss over in this essay.

[7] For a fuller description of the Clipper chip and a discussion of the constitutional issues raised by any attempt to legislate domestic controls on the use of encryption, see A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U Penn L Rev 709 (1995).

orchestrated by the United States government, that might result in transnational controls on the use of strong cryptography by both citizens and enterprises. Part IV, the conclusion, returns to the subject of trust and discusses Congress's role in the formation of a national cryptography policy. A postscript added shortly before this Article went to press offers a preliminary anlysis of some features of the Clinton Administration's October 1996 encryption proposal.

Overall, this Article aims to describe the issues in a rapidly changing and complex legal and technical debate. It also identifies significant legal and technical issues that current government proposals do not resolve. Rather than attempt to prescribe the content of a solution, however, the prescriptive portion concentrates on policy-formation procedures likely to be conducive to a resolution of the debate.

A. Goals and Challenges for U.S. Crypto Policy

For the past two decades or more, a major goal of U.S. cryptography policy—to the extent that the U.S. has had one[8]—has been to prevent strong mass-market cryptography from becoming widely available abroad, with export controls being the primary tool used to achieve this end. Primary responsibility for determining export-control policy fell to the National Security Agency, which determined policy in part in consultation with other participants in the Coordinating Committee for Multilateral Export Controls ("COCOM") group.[9] At home, the government has pursued a more schizophrenic policy, seemingly torn between embracing the benefits of cryptography for domestic security and the national economy,[10] while simultaneously being

---

[8] The "goals of U.S. cryptography policy have not been explicitly formalized and articulated within the government." *CRISIS Report* at Part II (cited in note 1); see also id at xiv (statement by Kenneth Dam noting absence of national policy).

[9] U.S. Department of Commerce and National Security Agency, *A Study of the International Market for Computer Software With Encryption* II-2 (1996) ("*Export Study*"). COCOM disbanded in 1994.

[10] For example, in 1977 the U.S. government adopted the Digital Encryption Standard ("DES") as a cipher certified as sufficiently strong for domestic business use. DES, issued as FIPS ("Federal Information Processing Standard") 46 in January 1977, was reviewed, slightly revised, reaffirmed for federal government use in 1983 and 1987, and reissued as FIPS 46-1 in January 1988; on September 11, 1992, the National Institute of Standards and Technology ("NIST") announced a third review of FIPS 46-1, DES, and reaffirmed it for another five years as FIPS 46-2. See Revision of Federal Information Processing Standard (FIPS) 46-1 Data Encryption Standard (DES), 58 Fed Reg 69,347, 69,347-48 (1993). Export of DES remains controlled under the ITAR to this day, which

unwilling to accept that the natural consequence of this policy is a reduction in the wiretapping and electronic investigatory powers of the law enforcement and intelligence agencies. These conflicting goals culminated in an unsuccessful attempt to convince the public to accept the Clipper chip, a device that offered the user superior encryption capabilities at the price of ensuring continued government access to encrypted communications.[11]

Although the Clipper chip failed to catch on, the long-term policy of which it is a part seems to have accomplished at least its objective of playing for time. Export control rules have had an effect on the domestic market for products with cryptographic capabilities such as e-mail, operating systems, and word processors. Largely because of the ban on export of strong cryptography, there is today no strong mass-market standard cryptographic product within the U.S. even though a considerable mathematical and programming base is fully capable of creating one. Windows 95, for example, does not come with cryptographic capabilities.

There are many cryptographers and computer hardware and software vendors outside the U.S., but U.S. companies such as Microsoft have large and often dominant market shares in important world markets: notably operating systems, word processors, e-mail systems, spreadsheets, and groupware.[12] A policy that affects the U.S. software industry thus has world-wide consequences which are felt at home as well as abroad. Export controls are ostensibly aimed only at foreigners. There are no legal restrictions on the domestic purchase or use of strong cryptography by U.S. citizens and permanent residents.[13] But by preventing the export of strong cryptography, the government slows its domestic use because many U.S. software vendors are reluctant to produce different domestic and export versions of their products.[14] Most manufacturers profess to believe that foreign customers will resent, and perhaps reject, a "crippled" export version

---

means that anyone seeking to export a DES product needs permission. Banks and other U.S. corporations seeking export clearance for DES products for internal use routinely receive export permission.

[11] See Froomkin, 143 U Penn L Rev at 744 (cited in note 7).

[12] See *Export Study* at ES-2 (cited in note 9) (noting that the "overwhelming majority (75%) of general-purpose software programs . . . available on foreign markets today are of U.S. origin").

[13] The Arms Export Control Act requires manufacturers of "munitions" (which are defined to include cryptography) to register with the State Department. 22 USC § 2778 (1988 & Supp IV 1992).

[14] See *Export Study* at V-4 (cited in note 9).

of a product and say they therefore choose to have one standard version for all countries.[15] Software makers wish to minimize the number of versions of their products so as to make maintenance and upgrading as simple as possible. As a result of these commercial and practical constraints, the U.S. mass market has ended up with the same relatively weak cryptography that the U.S. government permits to be exported.

Cryptographic algorithms ordinarily use a key to encrypt a message. Standard, single-key ciphers use the same key to encrypt and decrypt a message. Some modern public-key ciphers use two keys, each of which encrypts messages that can only be decrypted by the other. All other things being equal,[16] the strength of a secure cryptographic algorithm is proportional to the length of the key used to encrypt messages, a figure that is usually expressed in bits. Data Encryption Standard ("DES"), the official U.S. encryption standard, which is not freely exportable but has for some time been the de facto international standard also, uses fifty-six-bit keys, although there is reason to doubt that DES is sufficiently strong to prevent a reasonably determined attacker with a fast computer from decrypting a DES message in minutes.[17] The domestic versions of Netscape World Wide Web browsers use one hundred twenty-eight-bit keys when in secure mode. In contrast, the export versions of Netscape use relatively weak, forty-bit encryption because longer keys would require an export license.[18]

---

[15] "[T]he market reality is that a side-by-side comparison of two products identical except for their domestic vs. exportable encryption capabilities always results in a market assessment of the stronger products as providing a 'baseline' level of security and the weaker one being inferior, rather than the weaker product providing the baseline and the stronger one being seen as superior." *CRISIS Report* at 315 n 6 (cited in note 1); but see remarks of Ray Ozzie, http://www.lotus.com/notesr4/ozzie.htm (Jan 17, 1996) (describing "Differential Workfactor Cryptography" in which export editions of Lotus Notes are shipped with sixty-four-bit encryption enabled, but with twenty-four-bits encrypted in a LEAF-like data tag accessible to the U.S. government; as a result, the government need do no more brute-force work to decrypt the message than would be needed for a message using forty-bit encryption).

[16] For a discussion of the things assumed away in this magic phrase, see generally Bruce Schneier, *Applied Cryptography* (John Wiley & Sons, 2d ed 1996).

[17] See, for example, Matt Blaze, et al, *Minimal Key Lengths For Symmetric Ciphers To Provide Adequate Commercial Security*, http://www.bsa.org/bsa/cryptologists.html (Jan 1996) (stating that "U.S. Data Encryption Standard with 56-bit keys is increasingly inadequate").

[18] *CRISIS Report* at 4-11 n 24 (cited in note 1). For a discussion of the forty-bit limit, and the various demonstrations of the amount of computer power required to brute-force decrypt messages encrypted with forty-bit keys, see *The RSA Encryption Page*, http://www.library.carleton.edu/studentworkers/dan/rsa.html.

B. Export Control: The ITAR

The export of strong cryptographic tools from the U.S. is governed by the International Traffic in Arms Regulations ("ITAR").[19] The ITAR control the export of items listed on the U.S. Munitions List ("USML") and are administered by the Office of Defense Trade Controls in the Department of State. The Commerce Department administers the Export Administration Regulations ("EAR"), which regulate the export of so-called "dual-use" items listed on the Commerce Control List ("CCL").[20] Products offering data authentication, password protection, and access control are usually listed on the CCL. As an initial matter, products capable of encrypting a message are listed on the USML unless the product is restricted to financial uses such as ATMs. However, the State Department has the authority to transfer jurisdiction over export applications for any encryption product to the Commerce Department, and sometimes does so in a Commodity Jurisdiction ("CJ") determination, if it determines that the product no longer needs case-by-case review. Products that fall under the EAR can be exported under a general license; products that fall under the ITAR need a separate license application and review which ordinarily involves a referral to the Defense Department and the National Security Agency. The State Department routinely transfers jurisdiction over cryptographic products that use keys of forty bits or less to the Commerce Department "after a one-time review to ensure that the algorithm is implemented properly."[21] Exactly why the threshold is set at forty bits is unclear. "Most likely, it was the result of a set of compromises that were politically driven by all of the parties involved."[22]

---

[19] See 22 CFR § 121.1 (XIII)(b)(1) (1994). The statutory authority for the ITAR is the Arms Export Control Act, codified as amended at 22 USC § 2778 (1988 & Supp IV 1992). For a thorough survey of the ITAR and associated regulations, see Fred Greguras, *Regulation Update on U.S. Software Exports*, http://www.graphcomp.com/info/crypt/us_regs.html.

[20] The statutory authority for the EAR is the Export Administration Act of 1979, 50 USC app §§ 2401-2420 (1988 & Supp. IV 1992), which lapsed on August 20, 1994. See 50 USCA 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 Economic Powers Act ("IEEPA"), 50 USC §§ 1701-1706 (1988 & Supp IV 1992). See Continuation of Export Control Regulations, Exec Order No 12924, 59 Fed Reg 43437 (1994). President Clinton recently extended the state of emergency required to activate his authority under IEEPA; see Continuation of Emergency Regarding Export Control Regulations, 61 Fed Reg 42527 (August 15, 1996).

[21] See *Export Study* at II-1 to II-2 (cited in note 9).

[22] See *CRISIS Report* at 122 (cited in note 1).

Under the current ITAR regime, applications to export cryptographic software designed to encrypt messages with keys stronger than forty bits are generally denied, although authentication products that cannot be adapted for encryption, or which are designed for specific favored applications such as banking, tend to receive official export clearance.[23] Applications to export DES,[24] which uses fifty-six-bit encryption, are also often denied.[25] Applications for stronger products are considered to have little chance of approval. In theory, export controls are intended to prevent foreigners from acquiring cryptographic systems that are strong enough to create a serious barrier to traffic analysis, or that are difficult to crack.[26] In practice, although the ITAR have failed to prevent the spread of strong cryptography—algorithms and software created in the United States routinely and quickly find their way abroad, and foreigners create their own—the ITAR are widely considered to have prevented the emergence of a mass-market, international standard, cryptographic product.[27]

Indeed, uncertainty as to whether a given cryptosystem would be approved for export discourages software manufacturers from including strong cryptography.[28] The conventional wisdom in the highly competitive software industry holds that any delay may be fatal to a new product's marketability.[29] Routine export applications are approved quickly, but an ambitious application can meander though the administrative appeals process.[30] Since the government's objection to the export of products using keys in

---

[23] See Office of Technology Assessment, Congress of the United States, *Information Security and Privacy in Network Environments* 154 (1994); see also U.S. General Accounting Office, *Communications Privacy: Federal Policy and Actions* 6-7, 24-28 (1993).

[24] See Froomkin, 143 U Penn L Rev at 735-38 (cited in note 7) (discussing how DES became a standard in the United States). Exports to Canada are not controlled.

[25] See, for example, Trusted Information Systems, Press Release, *TIS Gauntlet™ Firewall with 56-bit DES approved for U.S. Export*, http://www.tis.com/docs/corporate/press/vpnpr.html (stating that TIS is first company to get U.S. export permision for DES-based firewall product).

[26] See Susan Landau, et al, *Codes, Keys and Conflicts: Issues in U.S. Crypto Policy* 25 (Association for Computing Machinery, 1994) ("*ACM Report*").

[27] See *Export Study* at III-9 (cited in note 9); *CRISIS Report* at 128 (cited in note 1).

[28] *Export Study* at V-4 (cited in note 9); *CRISIS Report* at 301 (cited in note 1).

[29] See generally Tracy Kidder, *The Soul of a New Machine* (Little, Brown, 1981); Douglas Coupland, *MicroSerfs* (Harper Collins, 1995).

[30] The record in *Karn v United States*, 925 F Supp 1 (D DC 1996) (appeal docketed) provides one, perhaps extreme, example. Karn submitted his original export request on Feb 12, 1994 and did not emerge from the appeals process with a final decision until June 13, 1995. Id at 2-3. See also *Export Study* at V-4 (cited in note 9) (citing two-year lead time to produce new products).

excess of forty bits, for other than specified exceptions such as banking or data authentication, is well known in the industry, many firms do not bother even to apply, and simply produce products they know can be exported.[31] U.S. producers of cryptographic software have become so cynical about the government's export policy that many declined to respond to a government survey designed to measure the extent of their concern about export control "because they were skeptical of efforts by the Government to accomplish anything of value related to encryption."[32]

The ITAR are controversial, and suits to have them declared unconstitutional as applied to the export of cryptographic source code have been filed in district courts in California and Washington, D.C. The California court held that an algorithm expressed in source code is protected speech,[33] a ruling that seems to lead inexorably to a decision that the ITAR are unconstitutional. The D.C. court dismissed a similar claim on political question grounds, and the decision is currently being appealed to the D.C. Circuit.[34]

While challenges to the ITAR wend their way towards the Supreme Court, technical and political developments are conspiring to make current U.S. export-control policy obsolete. The ever-increasing speed and number of computers make it increasingly cheap and easy to use brute-force methods to decipher messages encrypted with any given key length. Longer and longer keys are thus needed to achieve consistent levels of security, making the forty-bit limit on freely exportable cryptography increasingly obsolete. The accelerating digitization of the world increases the importance of information security. Meanwhile, U.S. dominance of the supply of strong cryptographic hardware and software may be about to disappear.

Against this background, the Clinton Administration has labored mightily to preserve what it can of the data acquisition capabilities of law enforcement and intelligence agencies.

---

[31] See *Export Study* at ES-4 (cited in note 9) (noting that companies "avoid [ ] applying for export licenses"); id at V-4.

[32] Id at V-1.

[33] See *Bernstein v. United States Department of State*, 922 F Supp 1426 (ND Cal 1996). Further information about this case is available online at http://www.eff.org/pub/Privacy/ITAR_export/Bernstein_case/.

[34] *Karn*, 925 F Supp 1 (cited in note 30). For full information, including all unsealed motions, pleadings and evidence, see http://www.qualcomm.com/people/pkarn/export/.

I. THE CLIPPER CHIP: TECHNICAL AND BUREAUCRATIC INNOVATION

With the Clipper chip the United States government hoped it had solved the encryption policy dilemma. The government introduced Clipper with an inventive strategy to manipulate information-processing standards, circumvent both Congress and the Administrative Procedure Act ("APA"), and rig the market for encryption devices. Despite this, the strategy failed when the public refused to buy or use the product. A companion product, the Capstone Chip implemented in the Fortezza card,[35] has fared somewhat better, but is far from market dominance.

In an effort to ensure the continuation of its law-enforcement-related searching and wiretapping abilities and its espionage-related electronic-eavesdropping capabilities, the government devised the Clipper chip[36] for secure telephones and the Capstone Chip-based Fortezza PCMCIA card[37] for secure e-mail and file encryption. Use of the chips was and is voluntary: U.S. citizens remain free to use any cipher they wish, so long as the software or hardware remains in the U.S. In February 1996, about two years after the Administration originally promised to promulgate a personal use exception, it became legal to take strong cryptographic programs abroad, on a laptop computer for example, for personal use.[38] It continues to be illegal to give or sell strong cryptography to foreigners without first obtaining an export license, which can be difficult or impossible to obtain.[39] However, U.S. law currently imposes no restriction on sending encrypted messages abroad, regardless of the strength of the encryption. The ITAR prohibit the export of the means to encrypt messages, not the messages themselves.

---

[35] Originally available only as a PCMCIA card, Fortezza now comes in an ISA variety as well. See *Fortezza CryptoSecurity Products*, http://www.rnbo.com/PROD/CRYPTO.HTM. A Quicktime Movie of a "virtual Fortezza Card" is offered by Rainbow Technologies, available online at http://www.rnbo.com/FORTVR.HTM (1996).

[36] The Clipper chip is defined—to the extent it has ever been publicly defined—in the Escrowed Encryption Standard ("EES"). See Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard ("FIPS 185"), 59 Fed Reg 5997 (1994). I discuss the original Clipper chip proposal in A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U Penn L Rev 709 (1995) (cited in note 7).

[37] See Froomkin, 143 U Penn L Rev at 715 n 16 (cited in note 7).

[38] See 61 Fed Reg 6111 (Feb 16, 1996) (personal use exception to ITAR). The regulations, however, impose surprisingly extensive record-keeping requirements on anyone who takes an encryption program to a foreign country. See id.

[39] See note 25 and accompanying text.

In both Clipper and Capstone, the government offered the public a carrot and a catch. The carrot was that both chips use SKIPJACK, a classified symmetric-key[40] encryption algorithm[41] with an eighty-bit key. SKIPJACK is certified as reliable by the NSA and is probably stronger than any alternative using a comparable key length; given its longer key length, SKIPJACK is certainly much stronger than the most widely used symmetric-key cipher, fifty-six-bit DES.[42] Market pressure for a substitute for DES is building because the cipher is now widely believed to be too weak for high-security applications due to advances in computer processing power,[43] although DES remains appropriate when very top-quality security is not required.

The catch in Clipper/Capstone was that the government would keep a copy of the keys—the unique codes belonging to each chip—thus allowing it to retain the ability to intercept every message sent using the chip. The government set out relatively elaborate procedures that it said would reduce the risk that the keys would be released to law enforcement agencies without legally sufficient justification, such as a valid wiretap authorization,[44] but the long-term efficacy of these procedures was debat-

---

[40] In a symmetric-key system both sender and receiver use the same key to encrypt and decrypt messages. In *public-key systems* the sender encrypts messages with a key that permits decryption only by a different key. Symmetric-key ciphers tend to work much more quickly than public-key ciphers of equivalent key length, and are thus more suited to real-time applications such as telephones, or to long documents. Symmetric-key systems rely on users safeguarding the key—if an interloper gets hold of the key he can decrypt all the messages encrypted with it. In contrast, public-key systems are more flexible, since one half of the *key pair* is secret and the other half can be made public. A message encrypted with the public key can only be read by the holder of the private key; if a message is encrypted with the private key, anyone who has access to the public key can read it, but the fact that the public key successfully decrypted the message authenticates it as emanating from the holder of the private key. Froomkin, 143 U Penn L Rev at 890-94 (cited in note 7).

[41] An algorithm is a more formal name for a cipher. An algorithm is a mathematical function used to encrypt and decrypt a message. Modern algorithms use a key to encrypt and decrypt messages. The number of possible values of a key is called the keyspace.

[42] See Gilles Garon & Richard Outerbridge, *DES Watch: An Examination of the Sufficiency of the Data Encryption Standard for Financial Institution Information Security in the 1990s*, Cryptologia 177 (July 1991) (stating that since its adoption in 1977, DES "has become the most widely used cryptographic system in the world"). A panel of eminent cryptologists selected by the government concluded that SKIPJACK should remain secure against brute-force attacks, despite continual increases in computing power, for at least thirty years. See Ernest F. Brickell, et al, *SKIPJACK Review Interim Report: The SKIPJACK Algorithm* 1 (July 28, 1993) (available online at http://www.quadralay.com/www/Crypt/Clipper/skipjack—review.html) ("[T]here is no significant risk that SKIPJACK will be broken by exhaustive search in the next 30-40 years."). The panel never issued a final report.

[43] See, for example, Blaze, et al, *Minimal Key Lengths* (cited in note 17).

[44] The procedures for creating and storing the chip keys in a secure manner are

ed. Whatever their technical merits, the government's proposals for safeguarding the keys remained vulnerable to a change in administration policy. The procedures were not based on any specific legislative authorization. The agencies that issued the relevant rules described them as procedural rules, not substantive rules, and issued them without APA notice and comment. As a result, the government retained the absolute right to change the rules at any time, perhaps without public notice.[45]

The Clipper/Capstone proposal was notable for both technical and bureaucratic innovations. The two most important technical innovations, other than SKIPJACK itself, were the reliance on "tamperproof"[46] hardware to make it difficult to reverse engineer a chip and construct rogue Clipper telephones or Fortezza PCMCIA cards,[47] and the construction of "escrow" protocols for the Clipper and Capstone chips. The bureaucratic innovations were at least as significant. In the process of bringing forward the Clipper proposal the federal government defined a federal information processing standard that didn't describe a standard, circumvented both Congress and the Administrative Procedure Act, and attempted to use government market power to create a de facto standard because no statute gave it the authority to create a mandatory standard.

A. Key "Escrow" in Clipper

The Clipper chip makes it possible for the government to decrypt a telephone call encrypted with a Clipper telephone by putting essential information into "escrow." The use of the term escrow is a misnomer, since the "escrow" is for the benefit of law

---

described in Dorothy E. Denning & Miles Smid, *Key Escrowing Today*, IEEE Comm 58 (Sept 1994) (available online at http://guru.cosc.georgetown.edu/~denning/crypto/clipper/Key-Escrowing-Today.txt).

The three sets of procedures for disclosure of keys for use in authorized federal, state, and national security-related wiretaps appear in Office of the Press Secretary, The White House, *Key Escrow Encryption: Announcements-February 4, 1994* (Feb 15, 1994) (information packet accompanying press release) (on file with the *Legal Forum*).

[45] See Froomkin, 143 U Penn L Rev at 763 (cited in note 7).

[46] See id at 753 n 187 (discussing tamperproof hardware).

[47] The dependence of Clipper and other products on "tamper resistant" hardware has spawned a cottage industry of attempts to subvert such schemes. Notable efforts include Yair Frankel & Moti Yung, *Escrow Encryption Systems Visited: Attacks, Analysis and Designs* in *Advances in Cryptology—CRYPTO '95 Proceedings* (1995) (on file with *The Legal Forum*, in which the authors describe a practical-sounding method of tricking a Clipper chip into using another chip's LEAF).

enforcement, not the parties to the communication, but the term has achieved wide currency, and we seem to be stuck with it.[48]

Escrow in Clipper works as follows.[49] Every Clipper chip bears a unique serial number and has a unique encryption key (the "chip-unique key") that is burnt in by the manufacturer under secure conditions.[50] The chip-unique keys are split into two pieces with each half held by an "escrow agent." Currently the two escrow agents are NIST, in the Department of Commerce, and the Treasury Department's Automated Systems Division.[51]

When Alice initiates a secure Clipper communication with Bob, the two Clipper chips first agree on a one-time *session key*[52] for the communication. They then exchange Law Enforcement Access Fields ("LEAFs"), a stream of bits that carries the data law enforcement would need to get access to the session key for that telephone call. To prevent "rogue" encryption, Clipper chips will not communicate with each other until they exchange valid LEAFs.[53]

Clipper would be worthless if unauthorized users could use the LEAF to defeat the Clipper chip. To prevent this, the session-key data in the LEAF is itself buried under two layers of encryption. First, the chip encrypts the session key with the chip-unique key. Then the chip appends its unique serial number and a checksum, and re-encrypts the entire data set with the *family key*, a key common to all Clipper chips, but—in theory—known only to authorized law enforcement personnel.

---

[48] For a technical survey of the types of "escrowed" encryption systems developed, see Dorothy E. Denning & Dennis K. Branstad, *A Taxonomy for Key Escrow Systems*, 39 Comm ACM 34, 36 (March 1996) (table entry for Fortezza card); Dorothy E. Denning, http://www.cosc.goergetown.edu/~denning/crypto/appendix.html.

[49] For a more detailed description of the Clipper chip's workings, see Froomkin, 143 U Penn L Rev at 753-59 (cited in note 7).

[50] For details, see Denning & Smid, *Key Escrowing Today* (cited in note 44).

[51] Office of the Press Secretary, *Key Escrow Encryption: Announcements* (cited in note 44).

[52] A session key is the sequence of bits allowing decryption that will be used for only a single communication, one e-mail, or one telephone call. Each time the parties initiate a new conversation, they generate a new session key, which, though lasting for the entire conversation, is never repeated. See Froomkin, 143 U Penn L Rev at 754-55 (cited in note 7).

[53] Matt Blaze's "LEAF-blower" exploited a vulnerability in the LEAF-checking algorithm to generate spurious approvals of counterfeit LEAFs. The method is too slow, however, to be of great practical value. See Matt Blaze, *Protocol Failure in the Escrowed Encryption Standard*, in *Building in Big Brother: The Cryptographic Policy Debate* 131 (Lance Hoffman ed, 1995).

Suppose that Louis, an FBI agent, has a Title III[54] judicial wiretap authorization[55] to monitor Alice's telephone calls. After recording the call and determining it to be Clipperized, Louis must obtain a special decrypt processor that has the family key. Louis can then use the processor to recover Alice's Clipper chip's serial number and the encrypted session key. Armed with the serial number and the appropriate legal authorization,[56] Louis can request that the two escrow agents give him the halves of Alice's chip-unique key; by putting these keys together, Louis is finally able to decrypt the session key and then decrypt the conversation.

Four aspects of this escrow procedure are particularly notable. First, both escrow agents must cooperate in order for Louis to be able to decrypt Alice's telephone call with Bob. So far as we know,[57] possession of the family key and half of the chip-unique key[58] is of no value in decrypting Alice's message. Second, once Louis has Alice's chip-unique key, he can use it to decrypt all of Alice's subsequent Clipperized telephone calls, overhearing both parties,[59] regardless of who Alice is talking to or which party initiated the conversation. Third, although the security of Alice's Clipperized telephone calls is permanently[60] compromised, Bob's

---

[54] Pub L No 90-351, tit III § 802, 82 Stat 197, 211-25, reprinted in 1968 USCCAN 237, 253 (current version at 18 USC §§ 2510-2521 (1988 & Supp V 1993)) ("Electronic Communications Privacy Act of 1986") (hereinafter "Title III").

[55] 18 USC § 2516 (1988 & Supp V 1993).

[56] Technically, Louis needs only to aver the existence of this authorization since the escrow agents have no obligation to make an independent confirmation of Louis's authority. They do, however, have an obligation to keep a record of who asks for what. See State Authorization Procedures at 1 (cited in note 44); Title III Authorization Procedures at 1 (cited in note 44); FISA Authorization Procedures at 1 (cited in note 44). The Department of Justice is required to ascertain, after the fact, that the legal authorization existed for Title III wiretaps and FISA wiretaps. See Title III Authorization Procedures at 2 (stating that the "Department of Justice shall" ascertain the existence of authorizations for electronic surveillance); FISA Authorization Procedures at 2 (same). The Justice Department has no such obligation when the key segment is requested by a state or local police force. See State Authorization Procedures at 2 (stating that the "Department of Justice may" inquire into the authorization for electronic surveillance).

[57] Since the SKIPJACK algorithm is classified, one cannot be more certain.

[58] A half key is not useful information because the two halves are XORed together to produce the actual key. See Froomkin, 143 U Penn L Rev at 759 (cited in note 7).

[59] Clipper does not work for conference calls.

[60] The specifications for the decrypt processor call for it to delete keys when a warrant expires and to automatically send a confirmation message to the key escrow agents. The interim model in use by law enforcement organizations in 1994-95 relied on manual deletion. See Office of Technology Assessment, *Information Security* at 65 n 5 (Box 2-7) (cited in note 23) (citing presentation by NIST Security Technology Manager Miles Smid in June 1994); that is to say, the model relied on trust.

communication security is unaffected, except when he talks to Alice, because Louis does not at any time have access to Bob's chip-unique key. Fourth, the federal escrow agents respond only to requests from authorized state or federal law enforcement or intelligence agencies. Even Alice herself cannot get access to her key if she needs it for some reason.[61]

B. Key "Escrow" in the Fortezza Card and the "Pile of Keys" Problem

The mechanics of key escrow in Fortezza have received considerably less attention than have the mechanics of Clipper. This is a pity because while Clipper has been reduced to a curiosity,[62] the Capstone-based Fortezza card has been adopted as the standard of the Defense Messaging System, giving it a projected installed base of two million users.[63] Capstone-based PCMCIA cards are in production and available for purchase by U.S. residents.

Fortezza and Clipper are similar in that both have a device-unique key that is used to generate a LEAF containing an encrypted version of the session key. This chip-unique key can be recovered from escrow by authorized government agents. But Fortezza has significant differences from Clipper because the Capstone Chip is designed to do different things from Clipper. While Clipper is exclusively for real-time encryption in telephones, a Fortezza PCMCIA card inserted into a computer can generate pseudo-random numbers, encrypt e-mail, and produce digital signatures.[64] In addition to the symmetric chip-unique

---

[61] Given that the Clipper chip is used only for communications, and not to archive stored information, this is not likely to be a serious problem for Alice; the application of the same rule is potentially significant for Fortezza escrow.

[62] See, for example, Jared Sandberg and Don Clark, *AT&T, VLSI Technology to Develop Microchips that Offer Data Security*, Wall Street Journal A3 (Jan 31, 1995) (noting AT&T abandoning Clipper chip).

[63] To date the NSA has issued solicitations for more than 750,000 Fortezza cards. Up to two million are expected to be in use by 2005. National Research Council, Kenneth Dam and Herb Lin, eds, *Cryptography's Role in Securing the Information Society* 177 (National Academy Press, 1996) (cited in note 1) (*"CRISIS Report"*).

[64] Public-key cryptographic systems allow users to append a digital signature to an unencrypted message. A digital signature encrypted with a private key uniquely identifies the sender and connects the sender to the exact message. Anyone who has the user's public key can then verify the integrity of the signature. Because the signature uses the plaintext as an input to the encryption algorithm, if the message is altered in even the slightest way, the signature will not decrypt properly, showing that the message was altered in transit or that the signature was forged by copying it from a different message. A digital signature copied from one message has an infinitesimal chance of successfully

key used by SKIPJACK to generate the LEAF, Fortezza also has other public/private keys that can be used for e-mail or for transmitting a SKIPJACK key to a correspondent. These public/private keypairs are not escrowed with the government but may be escrowed with a private company.[65]

The similarities between Fortezza and Clipper mask a substantial difference. If Louis, an FBI agent, has a Title III judicial wiretap authorization to monitor Alice's e-mail, he goes through steps identical to a Clipper request[66] to get access to Alice's *outgoing* e-mail. This procedure is of no value, however, if Louis wants access to Alice's *incoming* e-mail as well. The reason for this is a little complex, but it is important. When two Clipper chips want to communicate in real time, they agree on a session key,[67] which they both use for that telephone call. The LEAF-generation scheme used in Clipper relies on both chips knowing the session key, and on having both chips exchanging different LEAFs, each containing the session key. Thus, if Louis has a warrant allowing him to hear Alice's phone calls, Louis can recover the session key from *either* LEAF. Because the two Clipper chips work in synch, Alice's chip-unique key suffices to hear both sides of the conversation. E-mail doesn't work like that. When Bob sends an e-mail to Alice, his Capstone chip is not in direct communication with Alice, and his chip must therefore select the encryption key on its own.[68] As a result, although Bob's chip may send out a valid LEAF, it is not synchronized with Alice's chip, and Louis cannot be certain of making Alice's chip emit a LEAF containing the session key when she reads Bob's e-mail. It follows that unless Louis can somehow get access to Alice's private key the only way that he can read Bob's message is to also get the escrow agents to give him *Bob's* chip-unique key. If Alice gets lots of e-mail,

---

authenticating any other message. See Bruce Schneier, *Applied Cryptography* 35 (John Wiley & Sons, 2d ed 1996) (cited in note 16) (noting that a digital signature using a 160-bit checksum has only a one in 2^{160} chance of misidentification).

For a discussion of digital signatures and their importance to electronic commerce and electronic authentication, see A. Michael Froomkin, *The Importance of Trusted Third Parties in Electronic Commerce*, 75 Ore L Rev 49 (1996).

[65] See Denning & Branstad, 39 Comm ACM at 36 (cited in note 48).

[66] See note 52 and accompanying text.

[67] See id.

[68] If SKIPJACK is used to encrypt the e-mail, Bob needs a way to give the session key for that symmetric key system to Alice. He would probably use a public-private key system, in which he encrypted the session key with Alice's public key. When Alice receives the message, she will use her private key—which is not escrowed with the government—to decrypt the session key that SKIPJACK will accept as input to the decrypt function.

Louis may end up compromising a large number of Capstone chips' security, leading to the "pile of keys" problem.[69]

In summary, as in the Clipper chip case, both escrow agents must cooperate in order for Louis to be able to decrypt Alice's Capstone-encrypted e-mail. Also like Clipper, the federal escrow agents respond only to requests from authorized state or federal law enforcement or intelligence agencies. Unlike Clipper, Louis's possession of Alice's chip-unique key allows Louis to decrypt Alice's outgoing mail only, although it also gives Louis the ability to decrypt any messages Alice may have sent before the effective date of the intercept authorization if Louis can find copies of them. Unlike Clipper, in which both sides of the conversation could be heard, none of Alice's incoming mail is automatically affected. Unless Louis can get Alice's private key, which is not escrowed in the Fortezza scheme, the only way Louis can read Bob's encrypted e-mail to Alice is to get the escrow agents to give him *Bob's* chip-unique key. As a result, if Bob sends just one e-mail to Alice while she is the target of an investigation, Louis may be able to acquire his chip-unique key if the legal system allows him to get it from the escrow agents, which then gives Louis access to all of Bob's e-mail.[70] As with Clipper, Alice herself cannot get access to her key if she loses or damages her Fortezza card. Since e-mail is sometimes stored for long periods of time, this could be a more serious problem for Alice than was the exclusion of user access in Clipper.

C. Bureaucratic Innovation in the Clipper Plan

The Clipper chip affair produced a number of significant bureaucratic innovations. Each of these innovations appears to have derived from a common source: the absence of Congressional authorization for Clipper combined with a reluctance on the part of the executive branch to involve Congress in the cryptographic policy-making process.

---

[69] Whether the security of an encryption chip is actually compromised by the release of the chip-unique key to authorized law enforcement is a subject that polarizes debates between security professionals and law enforcement. Security professionals presume that security is unacceptably lessened whenever it is theoretically possible for third parties to gain access to keys; law enforcement officials tend to presume that the public should trust them.

[70] Using this access for anything other than mail to Alice without judicial authorization (or, perhaps, other authorization in the case of national security cases) would violate Title III.

Wielding market power to make policy. A stroke of bureaucratic genius lay at the heart of the Clipper strategy. Congress had not, and to this date has not, given the executive branch the power to control the private use of encryption. Congress has not even given the executive the power to set up an escrow system for keys. In the absence of any formal authority to prevent the adoption of unescrowed cryptography, Clipper's proponents hit upon the idea of using the government's power as a major consumer of cryptographic products to rig the market. If the government could not prevent the public from using nonconforming products, perhaps it could set the standard by purchasing and deploying large numbers of escrowed products. People who wanted to interoperate with the government's machines would naturally buy the same equipment. The existence of a large functioning user base would create further incentives for others to buy the same equipment, as would the existence of the federal government's imprimatur in a Federal Information Processing Standard ("FIPS").[71] Furthermore, bulk purchases by the government might drive down unit costs to the point that nonescrowed products might find it hard to compete.

Strange FIPS. Clipper was announced by means of a Federal Information Processing Standard, FIPS 185. FIPSs are standards and guidelines that are ordinarily intended to improve the federal government's use and management of computers and information technology, and to standardize procurement of those goods.[72] Formally, FIPSs apply only to the federal government and some contractors. A FIPS normally describes the device it covers in sufficient detail for the informed reader to distinguish a conforming device from a nonconforming device; indeed, FIPSs exist to provide that guidance. FIPS 185 was unusual in that rather than describing the essential, classified parts of the SKIPJACK encryption system or the LEAF creation method, FIPS 185 stated that conforming devices would be certified by the NSA.[73]

APA avoidance. Notice of a proposed FIPS is usually published in the Federal Register, with a request for public comments. The final version is also published in the Federal Reg-

---

[71] Mitch Ratcliffe, *Security Chips Trigger Alarm: Clipper and Capstone Open Digital Back Door*, MacWeek 1 (Apr 26, 1993) (stating that FIPS often become de facto standards because the U.S. government is the largest computer customer in the world).

[72] See Froomkin, 143 U Penn L Rev at 764-67 (cited in note 7).

[73] FIPS 185 at 6005 (cited in note 36).

ister. FIPS 185 was no exception. Notice and publication are not, however, required by statute.[74] The government argues that a FIPS is not within the class of rules to which the notice and comment procedure of section 553 of the APA[75] applies, and that was particularly true of FIPS 185 since it was, by its own terms, completely voluntary, even for federal agencies.[76] The formally voluntary nature of the standard was also used to justify the government's decision to refuse to address the concerns of commentators who understood that FIPS 185 was an attempt to coerce the public through market means.

It was a clever strategy. Nevertheless, the Clipper plan was unpopular from its inception and soon withered in the face of public opposition. Capstone on the other hand has had at least some success, albeit not enough to achieve the FBI's goal of ensuring that cryptography imposes no obstacle to law enforcement's legal efforts to acquire the content of electronic communications and stored data.

II. SOFTWARE KEY ESCROW

Even as Clipper was being unveiled in 1994, Vice President Gore suggested that the proposal might be modified to allow the export of cryptosystems in which keys were deposited with certified private escrow agents rather than directly with the government.[77] As it became increasingly clear that the Clipper plan would fail, the administration began to consult industry and other groups about a new proposal linking limited relaxation of export control with modified key escrow. The government called this revised plan "software key escrow,"[78] or sometimes "commer-

---

[74] See 40 USC § 759(d)(1) (1988) (requiring publication in the Federal Register only if President disapproves or modifies a FIPS).

[75] 5 USC § 553(b)-(d) (1988). NIST has traditionally followed a notice and comment procedure for FIPSs while maintaining that no statute actually requires it. But see *American College of Neuropsychopharmacology v Weinberger*, Food Drug Cosm L Rep (CCH) § 38,025 (D DC July 31, 1975) (holding that publication in the Federal Register combined with the complexity of the rules themselves meant that the rules in question were subject to the notice and comment procedures of section 553 of the APA).

[76] FIPS 185 at 5998 (cited in note 36).

[77] See Letter from Vice President Al Gore to Congresswoman Maria Cantwell (July 20, 1994) (available online at ftp://ftp.eff.org/pub/EFF/Policy/Crypto/Clipper/gore_clipper_retreat_cantwell_072094.letter). But see Statement of Patrick Leahy on Vice President Gore's Clipper chip Letter (July 21, 1994) (available online at ftp://ftp.eff.org/pub/EFF/Policy/Crypto/Clipper/gore_clipper_retreat_leahy.statement) (stating that the Gore letter "represents no change in policy").

[78] See *Draft Software Key Escrow Encryption Export Criteria*, http://csrc.ncsl.nist.gov/keyescrow/criteria.txt; *Key Escrow Agent Criteria*, http://csrc.ncsl.nist.gov/keyescrow/agent-

cial key escrow" ("CKE"),[79] but opponents dubbed it "Son of Clipper" or "Clipper II." Unlike Clipper, which relied on SKIPJACK, the software key escrow plan did not specify any particular encryption algorithm. Instead, the plan contained performance criteria designed to limit applications to at best medium-quality ciphers and to ensure that keys would be accessible when the government presented a lawful request. By mid-1996, however, several technical and political developments cast serious doubt on the viability of the proposal.

The software key escrow proposal combined the functions of *key archiving*, in which the owner of a key has emergency access to a backup copy of a lost key, with key "escrow," in which the government ensures that someone other than the keyholder has a copy of the key. If Bob has a copy of Alice's key, the government can serve a subpoena on Bob without tipping off Alice that she is the target of an investigation. Ensuring that the key is available from Bob means that the government has a way to decrypt Alice's data that is much easier than subjecting it to a "brute-force" decryption.[80]

One might ask why a foreign customer would be interested in a cryptographic product designed to be vulnerable to eavesdropping by the U.S. government. The government's proposal suggested that if suitable agreements could be negotiated with foreign governments, the escrow agents could be located abroad, under the control of a foreign government.[81] Although the proposal itself was silent on the likely content of foreign rules, it was possible to imagine circumstances in which a foreign government would favor escrowed encryption products, or even ban unescrowed encryption, in order to retain its eavesdropping capa-

---

criteria.txt.

[79] See *Draft Software Key Escrow Encryption Export Criteria* (cited in note 78); *Key Escrow Agent Criteria* (cited in note 78). The term "commercial key escrow" was something of a misnomer, since the proposal was neither commercial nor escrow as the terms are understood by most lawyers and business people. It was "commercial" only in the sense that the keyholders might be private firms rather than the government. It was not "escrow" in any ordinary sense of the word: usually, something held in escrow is held for the benefit of the owner. In software key escrow, as in Clipper, the "escrow" was for the benefit of the government rather than the owner of the key.

"Commercial Key Escrow™" (with capital letters) is a trademark of Trusted Information Systems.

[80] For a discussion of brute-force decryption, which is little more than trying every possible key until you find one that works, see A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U Penn L Rev 709, 887-89 (1995) (cited in note 7).

[81] *Key Escrow Agent Criteria* at ¶ 18 (cited in note 78).

bilities. Customers in such countries might have no choice but to buy an escrowed product if they wanted relatively strong, legal encryption.

In any event, nothing in the proposal would have allowed the export of products strong enough to defeat brute-force decryption by a determined government. The proposal contemplated allowing the export of products using ciphers with a key length of sixty-four bits or less, and only if the product also complied with other onerous criteria designed to prevent users from tampering with it to use unapproved algorithms. Each of these policies imposed significant burdens on the potential marketability of any product in addition to the fundamental problem that users would know they were buying a product designed to allow government access to their secrets. In particular, software makers desiring export clearance for products using encryption between forty and sixty-four bits would be required to:

(1) *Refuse to publish their source code.* This requirement is a significant obstacle to the sale of a security product because it means that outside experts are unable to verify the implementation of the algorithm. The proposal would have allowed firms to publish their algorithm and to publish input-output tables allowing users to check that the product really used the advertised algorithm, but these concessions were far from sufficient. There is much more to evaluating the security of an encryption system than merely proving that it uses DES instead of a simple letter substitution routine. For example, Netscape browsers were recently found to have a bug in their random number generators that resulted in predictable patterns in the numbers used to encrypt communications.[82] No test using an input-output table could detect this kind of error, but it is no less fatal.

(2) *Build in tamper-resistance.* The software would have to be designed to fail to run if users changed it in any way. This might have made upgrades more difficult.

(3) *Design a means of preventing multiple encryption.* The rationale for this requirement was to prevent a DES system from being used to produce 3-DES. In 3-DES a message is encrypted with DES using one key, decrypted with DES using a different

---

[82] See John Markoff, *Security Flaw is Discovered in Software Used in Shopping*, NY Times A1 (Sept 19, 1995); Netscape, *Welcome to Netscape Navigator Version 2.01*, available online at http://partner.netscape.com/eng/mozilla/2.01/relnotes/unix-2.01.html#Security (describing problem with implementation of random number generator and announcing bugfix).

key, and then re-encrypted using either the original key or a third key. 3-DES is considered much stronger than ordinary DES and is gradually replacing DES as a de facto international standard for high security civilian encryption.[83]

(4) *Ensure that the product refuses to communicate with unescrowed systems.* This feature alone would probably be enough to make the product uncompetitive unless unescrowed systems were very rare or unreliable.

Despite these enormous obstacles to commercial viability, the software key escrow plan was founded on the accurate observation that if businesses began to encrypt their data with strong ciphers, they would need some means to access that data in emergencies. Security professionals call this "key management," but they mean something that is not identical to key escrow. Wise key management involves ensuring access to copies of keys used in the course of business.[84] For a corporation encrypting its information, fail-safe access to critical data is essential. However, not all keys are equal. Access to the keys that safeguard corporate records might be more important than access to an employee's e-mail, although one could imagine circumstances, such as litigation, in which access to e-mail was necessary to reconstruct a transaction. Keys encrypting telephone conversations might be less important still, although even they might be useful if the firm imagines that it, or the police, might need to eavesdrop on employees in the course of an investigation of fraud or theft.

The software key escrow proposal extended to all keys used in communications, including telephones, but it did not involve the "escrow" of keys used in digital signatures. Indeed, escrow of digital-signature keys would be a very bad idea. For one thing, businesses would have little need to ensure emergency access to keys that give employees the power to do something because a well-designed key management system allows the appropriate authorities to revoke and create individuals' authorizations at will. For example, a corporation might issue digitally signed

---

[83] See Froomkin, 143 U Penn L Rev at 740-41 (cited in note 7).

[84] Since the person holding the keys can gut the security of the system if she does not hold the keys in a secure fashion, reasonable security may require that key fragments be distributed to two or more parties. In some systems the backup keyholders are not given the actual key to the cipher, but are instead entrusted with the key to a generic "data recovery field" encrypted into each message that contains the information needed to retrieve the key. The Clipper chip's LEAF, see note 52 and accompanying text, is an example of such a field.

certificates authorizing the holder of a digital-signature key to sign things in the corporate name or to transact up to a defined dollar limit.[85] Each digital-signature key is unique, and identifies the persons involved in the transaction just as much as it authenticates them as legitimate corporate representatives. A supplier presented with an employee's digital signature would ordinarily check to ensure that the certificate backing up that signature was valid before relying on it. This authentication usually requires a real-time check on the continuing validity of the corporate certificate.[86] If the employee's authorization lapsed for any reason, the corporation could easily revoke the certificate, making continuing authentication of the employee's digital signature impossible. As a result, a business using certificated digital signatures in its transactions would never need to forge an employee's digital signature, and would not want to create this capability for anyone else. The company retains control over delegated powers without needing to be able to pretend to be the employee.

Worse, "escrow" of a digital-signature key would tend to undermine one of the most important and useful features of a digital-signature system. So long as the user keeps control of her key, a message digitally signed by the user's key demonstrates beyond almost any doubt that the message was actually sent by that person and that it has not been altered in any way since it was signed. Admitting any challenge to the uniqueness of the signature would introduce a destructive element of doubt to this assurance, and would elevate the claim that a digital signature had been forged from the incredible to the conceivable. To its credit, the Administration recognized this and sought to exclude digital-signature keys from its key escrow proposal.[87]

Overall, the software key escrow plan sought to expand users' evident need for some sort of key archive in two directions that were less obviously in tune with users' interests. First the plan would have applied to encrypted communications, such as telephone conversations, as well as to stored data, although it was far from obvious that many would have chosen to archive keys used for communication rather than storage. Some compa-

---

[85] For a definition of a digital signatures, see note 64 and accompanying text. For a discussion of a digital-signature infrastructure and the role of certificates, see generally A. Michael Froomkin, *The Importance of Trusted Third Parties in Electronic Commerce*, 75 Or L Rev 49 (1996) (cited in note 64).

[86] See Froomkin, 75 Or L Rev at 82 (cited in note 64).

[87] But see note 168 and accompanying text.

nies might reasonably feel that they benefit from having the ability to eavesdrop on their employees. Some companies might reasonably conclude that they are better off if the government can easily investigate employees suspected of misdeeds. For these corporations, fraud prevention might be more important than employee and corporate privacy. Other companies might feel differently. Whatever the corporate view, individuals derive no direct personal benefit from making it possible for the government to tap their telephones, although society as a whole might gain some benefit from the increased effectiveness of law enforcement.

A. Who Holds the Keys

Because the person holding the "escrowed" key is capable of undermining the very security that a cryptographic security system is designed to create, the identity and duties of that keyholder are of paramount importance to anyone whose key is being held in this manner.

As originally formulated, the software key escrow plan appeared to assume that keys would be "escrowed" with an outside party.[88] Because one of the public objections to the Clipper proposal had been that the government would hold the keys, software key escrow contemplated that someone other than the government—a private escrow agent or the designer of the software—would be allowed to select a private "escrow agent." The plan was silent on critical questions, however, including:

- what security precautions commercial archives or commercial escrow agents would be required to offer;
- the liability of "escrow agents" in the event of
  - -the loss of a key;
  - -the compromise of a key, such as where the escrow agent's database is hacked or an employee is discovered to have sold key data;
  - -the good faith compliance with a facially valid but actually invalid warrant;
- under what circumstances a user could serve as his own escrow agent.

The liability issues were particularly difficult to deduce from the software key escrow proposal because it was unclear to what extent a user's participation in key escrow was truly voluntary.

---

[88] Key Escrow Issues Meeting, September 6-7, 1995, *Discussion Paper #4* § 10, http://csrc.ncsl.nist.gov/keyescrow/september_issues_mtg/paper4.html.

The more that the participation appeared coerced, the further the user-"escrow agent" relationship moved away from simple contract towards state action, and the murkier the liability questions became.

Indeed, the earlier Clipper proposal was notoriously silent on the duties and liabilities of the government escrow agents, leading all too easily to the conclusion that they would be difficult if not impossible to sue in the case of key compromise, and might effectively be accountable to no one. The Attorney General's escrow procedures for Clipper and Capstone state that they "do not create, and are not intended to create, any substantive rights for individuals intercepted through electronic surveillance."[89] In effect, the government disclaimed any reliance interest that a user of a Clipper telephone might have in the government's promise to keep the key secret.[90] A victim of an illegal wiretap would have a cause of action under Title III against the wiretapper,[91] but, it seemed, no remedy against the escrow agents, even if the escrow agents acted negligently or failed to follow their own procedures. If nothing else, this precedent suggested that liability rules should be of concern to potential users of key escrow.

Some of the concern over liability might have been alleviated by having private escrow agents take on contractual responsibilities; other answers might have resided in tort law, and still others might have emerged if the courts had considered the escrow agent to be a bailee or a trustee for the key's owner. In the absence of many functioning escrow agents, and in the complete absence of case law, there was at least considerable uncertainty as to what law governed an escrow agent. Worse, from the point of view of a business contemplating the use of an escrowed product, there was no reason to believe that an escrow agent would have sufficient assets to compensate the victim of unauthorized key disclosure for the potentially enormous damage that could be caused by the release of jealously guarded trade secrets and other corporate data.

Some businesses, especially smaller ones without their own security professionals, would likely have felt that they had less risk of unauthorized disclosure if they entrusted their backup

---

[89] Office of the Press Secretary, The White House, *Key Escrow Encryption: Announcements-February 4, 1994* (Feb 25, 1994) (cited in note 44) (on file with the *Legal Forum*).

[90] See Froomkin, 143 U Penn L Rev at 762 (cited in note 7).

[91] See 18 USC § 2520(a) (1994).

keys to outside professionals. Other firms, especially large multinationals with their own security staffs, might have made a different calculation and preferred to hold their own keys; they made this clear to the government when it published its first software key escrow proposal and asked for comments.

The government's response to these comments, unveiled in December 1995, was to clarify its objectives regarding the selection and certification of escrow agents. While agreeing that it would be "beneficial" to criminalize the "abuse of the escrowed key by the escrow agents or others,"[92] the proposal concentrated on the primary government objective of "assuring the availability of escrowed keys for properly authorized government officials" in a reliable and timely manner that would not tip off the subject of the investigation.[93] Recognizing that some organizations or people would want to be their own escrow agents, the proposal required that agents undertake to hold keys securely, and set out general requirements for the secure storage and transmittal of keys. More controversially, the proposal required that each escrow agent:

- employ one or more persons with a "SECRET" clearance;[94]
- provide a Dun & Bradstreet/TRW number or equivalent credit report pointer and authorization;[95]
- carry an errors & omissions insurance policy;[96]
- be primarily owned by U.S. citizens if located in the U.S.[97]

The draft candidly admitted that "[w]e have not yet addressed conditions under which users can be the sole repository of the keys for their system,"[98] although government speakers at the December NIST meeting indicated that they intended to allow suitable organizations able to comply with all the escrow-agent criteria to hold their own keys. In addition, although the government held out the possibility of foreign escrow agents, at least for foreign users, this possibility was contingent on negotiating appropriate agreements with each foreign government involved.

---

[92] *Key Escrow Agent Criteria* (cited in note 78). Irritatingly, all the government memoranda distributed at the 1995 NIST meetings on key escrow were handed out without advance notice, on paper with no letterhead. The memos bore no indicia of authorship.

[93] Id.

[94] Id ¶ 7.

[95] Id ¶ 13.

[96] *Key Escrow Agent Criteria* ¶ 14 (cited in note 78).

[97] Id ¶ 18.

[98] Id.

The requirement that escrow agents employ someone with a SECRET clearance—which had not been stated in the original software key escrow proposal—quickly engendered the greatest controversy, although taken as a group the other requirements were sufficiently burdensome to make it unlikely that any but a good-sized corporation could be its own escrow agent. Critics attacked the SECRET clearance requirement as a device the government could use to manipulate who it would allow to be an escrow agent. Others worried that the requirement could become a means by which the government could control agents' behavior, since agents could be threatened with a loss of their clearance if they did not do what the government wanted.

From the government's viewpoint, however, the SECRET clearance requirement was a necessary element of the key escrow strategy once it became clear that some escrow agents would be outside the government. Under federal regulations, wiretap and other orders issued by the FISA court are classified.[99] Thus, for example, federal law requires that telephone companies have someone on their staff with a SECRET clearance to receive and comply with FISA court-ordered wiretaps.[100]

B. Un-Commercial Key Escrow?

By late 1995, the software key escrow proposal had evolved to differ from Clipper in three important respects. First, the plan would allow the export of strong *software* encryption products, which made it broader and more acceptable to industry than the original Clipper proposal, which had been limited to hardware. Second, rather than allowing the export of the classified SKIPJACK algorithm provided for Clipper, which had an eighty-bit key, software key escrow products would be limited to sixty-four bit products.[101] The choice of algorithm was welcome, but the sixty-four-bit limitation made the proposal considerably less popular than it might otherwise have been. Third, the government would no longer demand that it hold the keys itself; instead, it offered to certify others to serve as private escrow agents in its stead. As we have seen, however, this offer soon proved to be less open-ended than it first appeared.

---

[99] See 50 USC § 1802(a)(4)(B) (1994) (authorizing Attorney General to classify fact of FISA order and to require that common carrier served with FISA order keep it secret).

[100] See id.

[101] *Draft Software Key Escrow Encryption Export Criteria* ¶ 7 (cited in note 78).

As with Clipper, the carrot held out to the software industry, and to users, was that the government might relax export controls. This was a powerful inducement since the ITAR regime imposed a de facto ban on the rapid export of encryption with more than forty-bit keys, and an all but impermeable ban on the export of ciphers stronger than fifty-six-bit DES. The stick was that the government demanded a computationally trivial, if not necessarily legally or procedurally trivial, means of gaining access to information encrypted by an exportable cipher by requiring that decryption keys, or the key fragments needed to reconstruct a key, be deposited with approved escrow agents.

Viewed from a charitable perspective, the software key escrow proposals floated in 1995 were simply cautious. Key escrow would guarantee the government access to encrypted information when it had a lawful order authorizing that access. As the government could get a copy of any escrowed key, it should have been indifferent to the key length. Despite the elaborate system designed to provide the government with the key, it continued to limit exportable cryptosystems to sixty-four bits. When asked why, government representatives would say only that they wanted to proceed with care, since they were not certain that parts of their proposed system, notably the attempt to design tamperproof software, would necessarily work in practice.

Viewed from a less charitable perspective, the conditions in the software key escrow proposal were onerous and uncommercial. The idea of escrow itself was loathed in some quarters. The sixty-four-bit limit was felt to be restrictive, especially when compared to 3-DES[102] and to IDEA, an increasingly popular 128-bit Swiss cipher. The requirement that escrow agents have a SECRET clearance was not perhaps as restrictive as it appeared, since these clearances are relatively easy to obtain, but the requirement tended to solidify the opposition of those suspicious of the escrow concept to begin with. Most, albeit not all, of the attendees at the NIST meeting in December 1995 who represented businesses wishing to export security products stated that they did not think the rules would allow them to export a commercially viable product.[103]

---

[102] See note 83 and accompanying text.

[103] A similar sentiment was voiced outside the meeting. See, for example, John Markoff, *Industry Group Rebuffs U.S. On Encryption*, NY Times D5 (Nov 8, 1995).

III. THE UNDEATH OF KEY ESCROW

Undaunted by the failure of Clipper and the rocky reception accorded software key escrow, the U.S. government returned to its strategy of looking for a lever with which to encourage or force the use of escrowed encryption. Using government market power to set a Clipper standard had failed. Using the carrot of relaxed export control to get software escrow did not seem to be taking the market by storm. Formally, both strategies remain in place, but neither seems likely to resolve the encryption dilemma. The new strategies for key escrow are, if anything, more subtle. On the one hand, the U.S. government now proposes to build escrow into the sinews of emerging networks of electronic commerce; on the other hand, the U.S. government is actively engaged with—or, some say, leading—foreign governments to set up international agreements that promote or require escrow as a condition of allowing transnational use of strong cryptography. The distinction between encouraging escrow and forcing escrow is significant, but the current policy is both evolving and opaque, making it unclear whether encouraging or forcing is the better word to describe the Administration's policy.

A. Evolution of the Key Escrow Debate

Four of the arguments frequently used by supporters of cryptographic export control were weakened, perhaps refuted, in the debates sparked by Clipper and software key escrow. The argument that existing rules allow the export of adequately strong cryptography was undermined by a report by a group of respected cryptographers. The argument that cryptographic export control imposes at most a minor burden on U.S. industry was challenged by a Department of Commerce study. The same study undermined the validity of the assumption that there are no serious foreign competitors for U.S. cryptographic products, as did the announcement of several new foreign sources of brand-name cryptography. Perhaps most importantly, the argument that there are good reasons, known only to those with access to highly classified information, why cryptography needs to be controlled, was decisively repudiated by the National Research Council's cryptography study.

1. *Key length.*

As computers become more powerful, longer and longer keys are needed to provide a consistent level of protection against brute-force attacks. This fact, more than any other, has created pressure to relax the ITAR. A recent report signed by seven leading cryptographers,[104] *Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security*, estimated that the forty-bit keys allowed by the ITAR "offer virtually no protection" today, that fifty-six-bit DES "is increasingly inadequate," and that "adequate protection" against "serious threats" requires at least seventy-five-bit keys.[105] The cryptographers calculated that a standard $10,000 computer could break forty-bit keys in an average of twelve minutes; a standard $10 million machine could do it in an average of less than a second; and optimized single-purpose machines could do the same job even faster and cheaper.[106]

Whether or not the *Minimal Key Lengths* conclusions are exactly right,[107] they are likely to be widely believed. As a result, the *Minimal Key Lengths* study is likely to shape the perceived security needs of commercial buyers of security products. These users will not be satisfied with fifty-six-bit DES for long, if

---

[104] The cryptographers were Matt Blaze, Whitfield Diffie, Ronald L. Rivest, Bruce Schneier, Tsutomu Shimomura, Eric Thompson, and Michael Wiener. See note 105.

[105] Matt Blaze, et al, *Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security*, http://www.bsa.org/bsa/cryptologists.html (Jan 1996).

[106] Id ¶ 3.

[107] One might quibble with these conclusions on two levels. Some argue that they are "threat estimates" rather than descriptions of actual capabilities today. Despite relatively conservative estimates of the capabilities of various existing hardware devices, the paper made little allowance for some practical difficulties with running a brute-force cracking device. In particular, the cryptographers' estimates begin with the standard assumption of a "known plaintext." This often, but not inevitably, accurate assumption is that at least part of the plaintext message sought to be decrypted is known to the attacker, perhaps because the message follows a standard form (such as a TO and FROM line in a memo). An attacker who lacks a known plaintext must devote extra computing time to deciding whether the text of each possible decryption of the message has an alphanumeric distribution consistent with ordinary language. This does not make brute-force decryption impossible, but it does slow it down.

Perhaps more telling, there is no public evidence that either businesses or law enforcement agencies have actually constructed a sophisticated brute force-decryption engine, much less employed it routinely. If they had, one might expect the information to leak eventually. Compare *US Cryptography Policy: Why We Are Taking the Current Approach*, http://csrc.ncsl.nist.gov/keyescrow/policy.txt (July 12, 1996) (suggesting that "operational reality" of government ability to decrypt messages greatly lags behind "mathematical theory").

Of course, anyone purchasing a security system today needs to build in sufficient security not just for the life of the system but, ideally, for the life of the data likely to be encrypted with that system. This requires a considerable margin for safety.

at all, and are likely to demand key lengths in the seventy-five-bit range suggested by the report in the near future. As a result, the government's willingness to relax the forty-bit limit to sixty-four-bits-plus-escrow in the software key escrow plan is likely to appear quite ungenerous.

2. *Effect on commerce.*

Encryption is becoming big business, with worldwide sales of encryption products estimated at $1.8 billion for this year. U.S. sales alone are estimated at just under $1 billion. Since a good fraction of this number is sales of hardware products, the software component represents only a small, but rapidly growing, part of the $77 billion world market for packaged software products.[108]

The Commerce/NSA study confirmed that foreign suppliers of encryption products are selling products advertised to use stronger algorithms, e.g. DES, than can be freely exported from the U.S.[109] Although the details were not released in the unclassified version of the report, the study suggested that these foreign implementations of DES were "not as secure as some U.S. products." Even so, the report stated, their existence "can have an effect on U.S. industry's competitiveness. . . . Some foreign encryption vendors reportedly use the existence of U.S. export controls on strong encryption to differentiate their products and capture markets from U.S. firms."[110]

While the foreign demand for encryption is still small, it is growing. The Commerce/NSA study demonstrated that U.S. firms were badly positioned to exploit this market despite dominance in the software industry, in large part because of export control or their self-censoring reaction to the controls. The conclusion that U.S. export controls can give foreign firms a competitive advantage was hardly surprising, but it added weight to the political case for relaxation of export control being mounted by the software industry.

---

[108] U.S. Department of Commerce and National Security Agency, *A Study of the International Market for Computer Software with Encryption* III-1, III-6 (1996) (cited in note 9) ("*Export Study*").

[109] Id at IV-1.

[110] Id at IV-3 to IV-4.

3. *Foreign sources of encryption technology.*

As we have seen, the de facto dominance of the U.S. computer industry has served as a critical component of the twin export-control and escrow advocacy policies of the U.S. government. Although foreign cryptographic products exist, none has been incorporated into a U.S.-made mass-market product. Furthermore, some of the best-known cryptographic products, such as the RSA encryption algorithm,[111] are themselves produced in the U.S. The absence of familiar brand names abroad has no doubt contributed to the slow spread of strong cryptography.

The cozy assumption that marketable cryptography does not breed outside the U.S. is suddenly less credible than it appeared to be even a year ago. First, reputable non-U.S. manufacturers such as Nippon Telephone and Telegraph have announced that they intend to produce strong cryptographic devices.[112] Second, U.S.-based companies have announced that they plan to *import* foreign cryptosystems and sell them under their own label.[113] Once in the U.S., strong foreign cryptography is no more exportable than the homegrown variety, but some U.S. companies apparently believe that they can structure their production so that non-U.S. clients would be served from offshore production sites and the goods would never fall within U.S. jurisdiction. Third, U.S. companies such as RSA are forming alliances with foreign cryptographers in which the U.S. tradename will be licensed to the foreign supplier.[114] The foreign product can be either indigenous or an indigenous implementation of an algorithm published in the U.S. since, at least at the moment, it is not an export-control violation to send encryption algorithms abroad in the form of equations printed on paper.[115]

---

[111] See generally RSA's *Frequently Asked Questions About Today's Cryptography*, http://www.rsa.com/yrsalabs/faq/faq_rsa.html (1993).

[112] See Testimony of RSA Data Security, Inc. President Jim Bidzos before the Senate Committee on Commerce, Science & Transportation, Subcommittee on Science, Space & Technology, 1996 WL 10828659 (June 12, 1996) (stating that NT&T is shipping encryption chips with 1024-bit RSA).

[113] For example, Sun Microsystems plans to import a Russian-built system for this reason. John Battelle, *Sun's Codemaking Comrades*, Wired 3.11 at 49 (Nov 1995).

[114] "RSA, which is based in Redwood City, Calif., plans to fund an effort by Chinese government scientists to develop new encryption software. The Chinese-developed software, based on RSA's general mathematical formula, may be more powerful than versions now permitted for export under U.S. laws, said James Bidzos, RSA's president." Don Clark, *China, U.S. Firm Challenge U.S. On Encryption-Software Exports*, Wall Street Journal A10 (Feb 8, 1996). For RSA's version of its alliance, see RSA, *RSA Data Security, Inc. and People's Republic of China Sign MOU on Encryption Technology and Joint Research*, http://www.rsa.com/rsa/china_rsa.htm (Feb 2, 1996).

[115] The State Department ruled that exports of the dead tree version of the book

4. *The CRISIS Report.*

On May 30, 1996, the National Research Council released a prepublication draft of *Cryptography's Role in Securing the Information Society* ("*CRISIS Report*"), emphasizing the cost to the United States of not having strong, widely deployed cryptography in an age of large information-security vulnerabilities that could affect important civilian applications. The Committee that authored the Report was drawn from leaders in national security, law, foreign relations, communications, and computer science. The Report is unusually thorough, containing a wealth of information on cryptography and cryptography policy, and its conclusions are likely to shape the cryptography debate.

Indeed, the Report's most important achievement may be that its existence legitimates debate. One argument sometimes heard in defense of key escrow and other controls on cryptographic technology is that "if you knew what we knew, you would agree with us."[116] The *CRISIS Report* decisively neutralizes that argument when it states that "the cleared members of the [National Research Council's Committee to Study National Cryptography Policy] (13 of its 16 members) concluded that *the debate over national cryptography policy can be carried out in a reasonable manner on an unclassified basis.*"[117]

The Committee's first recommendation is that "no law should bar the manufacture, sale, or use of any form of encryption with-

---

Applied Cryptography (1st ed) were not subject to the ITAR. *Letter from William B. Robinson, Director, Office of Defense Trade Controls, to Phil Karn*, http://www.qualcomm.com/people/pkarn/export/book-response.html (Mar 2, 1994). However, the US government's brief in *Karn v. United States*, 925 F Supp 1 (D DC 1996), appeal docketed, suggested that this ruling might have been a mistake. Defendants' Memorandum of Points and Authorities at § II B2i, available online at http://www.qualcomm.com/people/pkarn/export/memorandum.html (Nov 15, 1995). Judge Richie's ruling in the *Karn* case was sufficiently broad as to give comfort to a government official thinking of toughening the policy.

[116] National Research Council, Kenneth Dam & Herb Lin, eds, *Cryptography's Role in Securing the Information Society* ("*CRISIS Report*") xii (National Academy Press, 1996) (cited in note 1). As the Report notes,

> Such a position may be true or false, but it clearly does not provide much reassurance for those not privy to those secrets for one very simple reason: those who fear that government is hiding poorly-conceived policies behind a wall of secrecy are not likely to trust the government, yet in the absence of a substantive argument being called for, the government's claim is essentially a plea for trust.

Id.

[117] Id at 4 (emphasis in original).

in the United States."[118] As the committee noted, this recommendation conforms to current Administration policy, although this is an area where no administration can bind its successors.

On the question of whether the gains to national security from secure communications and data storage outweigh the losses to law enforcement and national security, the Report concludes that, "on balance, the advantages of more widespread use of cryptography outweigh the disadvantages."[119] The Report does not, however, recommend that the application of the ITAR to cryptography be discontinued. Instead, it recommends that export controls on cryptography "should be progressively relaxed but not eliminated,"[120] with most export control on fifty-six-bit DES being removed immediately so long as the products cannot be used to generate 3-DES.[121]

The decision to draw the line at DES has all the earmarks of a political compromise. The report lists six advantages of DES:

- DES offers a higher level of confidentiality than common forty-bit ciphers, one "adequate to promote broader uses of cryptography."
- DES is certified as secure by the U.S. government. The U.S. government's certification is due to expire in 1997,[122] and the Report notes that "future certification cannot be assured."[123]
- DES has been subjected to public scrutiny for more than twenty years and no one has found significant weaknesses in the algorithm.
- DES is in the public domain.
- DES has "nearly universal name recognition."[124]
- U.S. exporters need DES to be on a level playing field with foreign suppliers.

Notably absent from this list is any assertion that DES represents the user's optimal tradeoff between security on the one hand and financial and computer-processing cost on the other. Instead, the Committee says DES is "'good enough' for most information security applications and is likely to be good enough for the next decade, because only the most highly motivated and

---

[118] Id at 303.
[119] Id at 6.
[120] Id at 307.
[121] *CRISIS Report* at 312-13 (cited in note 1). On 3-DES, see note 83.
[122] See note 10.
[123] *CRISIS Report* at 315 (cited in note 1).
[124] Id.

well-funded organizations will be capable of sustaining brute-force attacks on DES during that time."[125]

In short, fifty-six-bit DES is a lot better than the forty-bit ciphers freely exportable today and was, in the Committee's judgment, the most that one could get. The Report forthrightly admits that "a replacement for DES will eventually be needed," but balances this with the statement that a move to widespread use of DES "may have a negative impact on the collection of signals intelligence"[126] albeit one that "has well-known and well-understood characteristics."[127] What this suggests about the U.S. government's ability to do brute-force decryption of DES messages is left to the reader's imagination.

As for encryption products stronger than DES, the *CRISIS Report* says that they should be allowed to approved end-users, but only when the end-user is willing to "provide access to decrypted information upon legally authorized request."[128] The recommendation leaves it open to the end-user to determine how to do this, although it notes that "many of them may well choose to use escrowed encryption products."[129]

The *CRISIS Report* also proposes that the U.S. government explore using escrowed encryption for internal purposes to "better understand how escrowed encryption might operate,"[130] and that the U.S. government should "work with other nations" in order to "address the critical international dimensions of escrowed communications."[131] Despite recommending that the U.S. government work out international escrow agreements and itself serve as an escrow testbed, the NRC committee concluded that "aggressive promotion" of escrowed encryption to the private sector "is not appropriate at this time."[132] It gave four reasons: First, too little is known about how to implement escrowed encryption to rely on it for a large-scale deployment. Second, because it is too easy to circumvent escrowed encryption schemes, it is unclear how valuable it would be. Third, technologies are changing so rapidly that imposing any system on the market would greatly distort progress in these areas. Fourth, it is un-

---

[125] Id at 316.
[126] Id at 317.
[127] *CRISIS Report* at 317 (cited in note 1).
[128] Id at 317-18.
[129] Id at 318.
[130] Id at 328.
[131] *CRISIS Report* at 328 (cited in note 1).
[132] Id at 329.

clear whether the market would accept escrow.[133] This conclusion—neither a rejection nor an endorsement of key escrow—has already proved controversial, as it pleased neither the proponents of escrow[134] nor its opponents.[135] It also had no effect on the Administration, which is forging ahead with its plans for escrowed systems.[136]

The *CRISIS Report* also makes a number of suggestions as to how the U.S. government could "assist law enforcement and national security to adjust to new technical realities of the information age." In particular it proposes that the U.S. government encourage the use of cryptography for user authentication, document authentication (digital signatures), and secure time stamps.[137] Each of these suggestions should be uncontroversial.

B. "Clipper III": a Proposal for an (Escrowed) Key-Management Infrastructure

At the close of the December 1995 Key Escrow Issues Meeting, NIST predicted that it would issue new guidelines setting out a relaxation in the export rules for software key-escrow products within a few weeks. The guidelines were then to be turned over to the State Department to implement, either as modifications to the ITAR regime or in some other manner.

More than six months later, neither a new FIPS nor a final draft of the interagency guidelines has yet appeared, suggesting that the interagency group directing export policy—which includes representatives from the FBI, NSA, NIST, and the Executive Office of the President—has been unable to agree on a firm policy. Instead, In May 1996, the Interagency Working Group on Cryptography Policy issued yet another trial balloon, in the form of a draft paper, *Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure* (the *"White Paper"*).[138] Its critics quickly dubbed it "Clipper III."

---

[133] Id at 329-33.

[134] See, for example, Dorothy E. Denning, *Comments on the NRC Cryptography Report*, http://guru.cosc.georgetown.edu/~denning/crypto/NRC.txt (June 11, 1996).

[135] See, for example, *EFF "Privacy-Crypto-Key Escrow & Govt. Access to Keys" Archive*, http://www.eff.org/pub/Privacy/Key_escrow/ ("Unfortunately, the report also calls for key 'escrow', and buys into the government's wacky idea of a federally-controlled 'Key Infrastructure', among other flaws").

[136] See note 140 and accompanying text.

[137] *CRISIS Report* at 324 (cited in note 1).

[138] Bruce W. McConnell & Edward J. Appel, Co-Chairs, Interagency Working Group on Cryptography Policy, *Draft Paper: Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure* 23 (May 20, 1996) (*"White Paper"*) (avail-

The policy sketched in the *White Paper* represents a significant departure from Clipper and software key escrow, and not only because for the first time the government made it clear that it was prepared to allow "export of products of any bit length" to foreign markets whose governments have legislated escrow requirements that are at least as comprehensive as the ones proposed for the U.S.[139] The *White Paper* also promises to allow self-escrow—but only for corporations, not individuals, and only so long as the escrow facility meets rigorous performance standards. The self-escrow standards repeat those proposed earlier for other escrow agents,[140] with the additional requirement that there be some guarantee that the person who would be replying to a request for keys would be someone other than the likely target of an investigation.

The most significant element of the new plan, however, is that instead of attempting to define standards for key escrow in hardware or software, the *White Paper* suggests that the government may attempt to require that escrow be built into the information infrastructure needed for secure electronic commerce. To fully appreciate the significance of the *White Paper's* attempt to use electronic commerce as the lever to promote key escrow requires some familiarity with public-key cryptography[141] and its use in electronic commerce.[142] In a public-key cryptosystem, messages encrypted with one key can be decrypted only with a

---

able from Office of Management and Budget, Executive Office of the President and available online at http://www.isse.gmu.edu/~pfarrell/nist/kmi.html).

The Administration reaffirmed its commitment to the policy outlined in the draft *White Paper* in a statement issued by Vice President Al Gore on June 12, 1996. See Statement of Vice President Al Gore, http://csrc.ncsl.nist.gov/keyescrow/admin.txt. See also John Markoff, *Clinton Proposes Initiatives On the Scrambling of Data*, NY Times 34 (July 13, 1996) (noting that administration was rejecting NRC recommendations); *US Cryptography Policy* (U.S. government policy paper issued July 12, 1996) (cited in note 107).

[139] See *White Paper* at 7 (cited in note 138).

[140] See notes 92-97 and accompanying text.

[141] Very compressed explanations appear in notes 40 (contrasting public-key cryptography with symmetric-key cryptography) and 64 (describing use of public-key cryptography to create a digital signature). Fuller explanations appear in A. Michael Froomkin, *The Metaphor Is The Key: Cryptography, The Clipper Chip, And The Constitution*, 143 U Penn L Rev 709, 890-94 (1995) (cited in note 7), and Bruce Schneier, *Applied Cryptography* (John Wiley & Sons, 2d ed 1996) (cited in note 16).

[142] On the use of cryptography in electronic commerce, see generally A. Michael Froomkin, *The Importance of Trusted Third Parties in Electronic Commerce*, 75 Or L Rev 49 (1996) (cited in note 64). On electronic commerce and electronic cash, see generally A. Michael Froomkin, *Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases*, 15 Pitt J L & Commerce 395 (1996).

different key, and vice-versa. A strong public-key system is one in which possession of both the encryption algorithm and one key gives no useful information about the other key and thus no clues as to how to decrypt the message.[143] The system gets its name from the idea that the user will publish one key, but keep the other one secret. The world can use the public key to send messages that only the private-key owner can read; the private key can be used to send messages that could only have been sent by the key owner.

Secure communications are a prerequisite to the exchange of sensitive commercial or financial information. Public-key cryptography allows Alice and Bob to establish a secure line of communication over an insecure medium, such as the Internet. First, Alice and Bob exchange the plaintext of their public keys. Then, Alice and Bob can each encrypt their outgoing messages with the other's public key and decrypt their received messages with their own secret, private key. All Alice and Bob need to communicate securely, therefore, is compatible encryption software and a secure means of consummating the initial exchange of public keys.

Alas, without some source of independent confirmation, Alice has no way of knowing whether an e-mailed key purporting to be from Bob is from Bob or from an imposter. [144](Bob has the same problem regarding Alice.) Thus, if Alice is prudent she will demand some assurance that she is not e-mailing the details of a tender offer or the PIN to her online bank account to a malicious stranger who might seek to profit at her expense; this need for assurance is one of the largest obstacles to widespread Internet-based electronic commerce.[145]

One means of providing assurance that a public key labeled as Bob's really belongs to him and no one else is to set up one or more secure registries of public keys, known as *Certification Authorities* ("CAs").[146] A CA might, for example, agree to list public keys in its secure registry only if the person supplying the key provides some identification to authenticate her claims about

---

[143] See Schneier, *Applied Cryptography* at 284-85, 318-20 (cited in note 16) (stating that security of public-key systems depends on inability to factor large numbers rapidly or on the continuing inability of mathematicians to solve the longstanding problem of calculating discrete logarithms).

[144] See id at 48-49 (describing "man in the middle" attack on secure communications).

[145] See Froomkin, 75 Or L Rev at 51-55 (cited in note 64).

[146] In addition to binding identities to keys, CAs may issue certificates attesting to some fact about a key or a transaction, or timestamps proving that a document was in existence at a certain time. A more extensive treatment of these functions, and of the duties and possible liabilities of CAs, appears in Froomkin, 75 Or L Rev 49 (cited in note 64).

her identity;[147] otherwise, someone might be tempted to deposit a public key in the name of Bill Gates and then try to purchase something expensive. Once the CA accepts Bob's identification (and, in most scenarios, charges Bob a small fee), the CA undertakes to supply a cryptographically unforgeable electronic certificate[148] attesting that "Bob's key" is really his.

Because the CA's certificate is digitally signed with the CA's private key, but is delivered by e-mail or via a World Wide Web page, Alice will need a reliable copy of the CA's public key to authenticate the certificate that certifies to the authenticity of Bob's public key. In effect, the problem of relying on Bob's key is transformed into the comparable problem of relying on the CA's key. This problem, however, is easier to solve because a CA, as a repeat player, will have a much greater interest than Bob in providing an out-of-channel means of authenticating its key. The CA might publish the text of its public key in the newspaper,[149] or the CA might arrange to have its public key delivered by a trusted intermediary. A list of public keys authenticated by the telephone company might, for example, be inserted into every telephone bill.

Another way for a CA to give Alice the confidence she needs is to have an identifying certificate from a second CA, certifying the first CA's key. CAs that certify other CAs are said to participate in a *certificate chain*, with a *root certificate* at the bottom of the tree.[150] Unfortunately, this just shifts the problem again, onto the validity of the root certificate. Unless a source can be

---

[147] The *White Paper* includes a misleading statement suggesting that the CA ordinarily would want or need to "escrow" the user's private key or other information that would allow access to the user's data or communications. In fact, none of the other models for a PKI includes this feature. See note 162 and accompanying text.

[148] A certificate is a computer-based record which (1) identifies the CA issuing it; (2) names, identifies, or describes an attribute of the subscriber; (3) contains the subscribers's public key; and (4) is digitally signed by the certification authority issuing it. Warwick Ford, *Advances in Public-Key Certificate Standards*, 13 SIG Security, Audit & Control Review at 9 (July 1995). See also Utah Digital Signature Act § 103, Utah Code Ann § 46-3-103(3) (1996).

[149] A printed public key is likely to be a long string of gibberish. To make life easier for the user, the CA probably would publish a short alphanumeric string, sometimes called a "key fingerprint," which could be checked against the electronic form of the full key. See Schneier, *Applied Cryptography* at 30-31 (cited in note 16).

[150] Ford, *Advances* at 9-10 (cited in note 148).

found for the root certificate that gets its trust from outside the insecure network, it is turtles all the way down.[151]

The *White Paper's* escrow proposal contemplates the federal government issuing the root certificate for a national Public-Key Infrastructure ("PKI"). CAs that meet licensing requirements would be rewarded with government certification of their keys. These CAs in turn would issue certificates to other CAs, and so on.[152] That the government might issue the root certificate is not especially controversial,[153] although it may or may not be of enormous practical significance unless backed by legislation if users prefer flatter certification hierarchies. Many certificates in the private sector might be self-signed or supported by at most one outside organization. The smaller the number of CAs involved in checking the validity of a certificate, the less effort required to confirm the validity of a certificate.[154] Of course, if participants in the government-certificate hierarchy receive valuable benefits, for example reduced exposure to liability for erroneous certificates,[155] every CA may want to have its key in a certification chain with the government at its root whatever the increased overhead costs. If federal legislation required that CAs be licensed and that a CA be in the government-backed certificate chain to be eligible for a license, then the government's prediction that users will choose a multilevel hierarchy would become a self-fulfilling prophecy.

---

[151] The canonical law review version of the turtle story goes as follows:

> William James described a classic encounter between scientific truth and a committment of faith. A prominent scientist had just given a brilliant lecture on the foundations of the universe. During the question period [a person] suggested that there was a problem with the professor's analysis. 'What is that?' asked the professor cautiously. 'It's all wrong,' [the person] replied, 'because the universe actually rests on the back of a giant turtle.' The professor, taken aback, forced a smile and then countered: 'If that's the case there is still the question, what is that turtle standing on?' The audience tittered, but [the person], undaunted, replied: 'Another, much larger turtle.' 'But . . . ' objected the professor. 'I'm sorry, professor, it's turtles all the way down.'

Roger C. Cramton, *Demystifying Legal Scholarship*, 75 Georgetown L J 1, 1-2 (1986).

[152] *White Paper* at Appendix I (cited in note 138).

[153] For example, the Utah Digital Signature Act contemplates that the state government will issue the root certificate for CAs licensed in Utah. See Utah Code Ann §§ 46-3-201(1), 46-3-201(2) (1996).

[154] See Froomkin, 75 Or L Rev at 54-61 (cited in note 64).

[155] The *White Paper* proposes legislation ensuring that CAs "who exercise due prudence" receive "liability protection." *White Paper* at 10 (cited in note 138). In the absence of such legislation the liability of CAs for erroneous certificates is complex, uncertain, and potentially large. See Froomkin, 75 Or L Rev at 82-85 (cited in note 64).

Some analysts suggest that as much as 15 percent of all consumer purchases may be electronic by the turn of the century,[156] but this is unlikely without an information infrastructure that enables secure communication and transactions.[157] Thus, the Interagency Working Group's suggestion that access to the PKI might be denied to users of unescrowed cryptography is of critical significance. In its starkest form, this proposal could amount to saying that any U.S. resident who refuses to submit to key escrow will be cut out of the emerging electronic market.

Whether the government intends such a stark result is uncertain, both because the *White Paper* is only a draft and because the report itself is unclear at key points. The *White Paper* offers principles that it asserts "need to be accepted by government, industry, and other users."[158] Some of these proposed principles are vague; others are certain to be controversial.

The *White Paper* proposes that the government promote the development of a PKI, but it makes key escrow the price of admission:

> To participate in the network a user needs a public key certificate signed by a CA which "binds" the user's identity to their public key. One condition of obtaining a certificate is that sufficient information *(e.g., private keys or other information as appropriate) has been escrowed with a certified escrow authority to allow access to a user's data or communications.*[159]

The italicized portion of this assertion is unique to the *White Paper*. No other proposal for a *public-key* infrastructure currently being discussed in the U.S. requires that all users divulge their private keys to a CA or anyone else.[160] On the contrary, while other proposals anticipate that users seeking an identifying cer-

---

[156] *Where E-Cash Will Take Off*, Business Week 70 (June 12, 1995). Another estimate suggests more than $200 billion in Internet commerce within five years. See John Kavanagh, *Purchases on the Internet Could Potentially Exceed $200bn by Year 2000*, Fin Times FT-IT XII (Nov 1, 1995) (quoting wide variety of estimates). Internet purchases in 1994 were estimated at $240 million. Id. See also Edward Mozley Roche, *Business Value of Electronic Commerce over Interoperable Networks*, Paper Presented at Freedom Forum, July 6-7, 1995, available online at http://www.commerce.net/information/reference/roche.txt (projecting huge increases in internet commerce).

[157] See generally Froomkin, 75 Or L Rev 49 (cited in note 64).

[158] *White Paper* at 3 (cited in note 138).

[159] Id at 5 (emphasis added).

[160] Examples include the ABA digital-signature guidelines and the various states' digital-signature legislation. See note 175 and accompanying text.

tificate will have to give the CA evidence of their identity so that the CA can issue the certificate in good faith, they also make it clear that the user has a duty to safeguard the secrecy of her private key.[161] The *White Paper* blurs the difference between showing a CA a passport or a corporate resolution granting signature authority to an individual, and giving an outside authority the ability to intercept all of one's communication.

The *White Paper* qualifies its general assertion that private keys must be divulged to the CA or an escrow agent with a footnote stating that it "applies only to keys used for confidentiality purposes and not keys used for signing purposes."[162] Indeed, no legitimate law enforcement or intelligence purpose could be served by giving the government or anyone else access to the digital-signature private keys belonging to either citizens or corporations.[163] A digital signature is appended to the cleartext of a message and uniquely identifies the author while unforgeably authenticating the text to anyone who possesses the corresponding public key. Giving Bob or Uncle Sam access to Alice's digital-signature key would allow them to impersonate Alice. As digital signatures become integrated into electronic commerce, a possessor of Alice's private digital-signature key will be able to empty her bank account, sign her name to contracts, and affix a signature she will be hard-put to disclaim to the most detailed "confession" of horrible crimes.[164]

The Interagency Working Group ("IWG") should be commended for recognizing that, whatever one thinks of the needs of law enforcement and others for access to the contents of encrypted communications, giving anyone a means of access to digital signature keys would undermine confidence in the uniqueness of the digital signature. Oddly, the IWG does not seem to have recognized that this essential caveat creates a technical problem that threatens to undermine the idea of an escrowed PKI. While it is true that *some* digital signature keys can be used only to sign documents, other algorithms including the RSA algo-

---

[161] See id.

[162] *White Paper* at 6 n 3 (cited in note 138).

[163] See notes 85-87 and accompanying text.

[164] See Froomkin, 75 Or L Rev at 108-110 (cited in note 64) (describing proposals to shift burden of proof so that digital signatures backed by a valid certificate will be presumed to have been affixed by person identified in the certificate). Digital-signature keys "must be controlled solely by the immediate and intended parties to those applications" because "outside access to such keys could undermine the legal basis and threaten the integrity of these practices carried out in the electronic domain." *CRISIS Report* at 326-27 (cited in note 1).

rithm,[165] which is the de facto industry standard, use keys that are equally effective for signing or encrypting documents.[166] The Interagency Working Group is left with a Hobson's choice. Either it plans to require escrow of every certificate-backed long, strong, key that can be used either for signing or encryption—and in so doing plans to reduce confidence in the uniqueness of signatures with RSA, one of the most widely used encryption algorithms—or it will allow the PKI to host nonescrowed digital-signature keys that can easily be used to subvert the escrow procedure.

A similar uncertainty as to the Interagency Working Group's actual goals emerges from the principle in its report that should be the least controversial: "Participation in the [key management infrastructure] will be voluntary."[167] Unfortunately, in the context of the entire *White Paper* it is difficult to understand whether the Interagency Working Group means anything more than the truism that no one will be forced to use public-key cryptography. It is particularly unclear whether the Interagency Working Group contemplates allowing alternate certificate hierarchies using strong cryptography to exist, and what burdens it hopes to place on any alternatives that survive.

The Interagency Working Group seems to believe that the nongovernmental, escrow-free certificate hierarchies currently being deployed by various private firms should not be allowed to exist beyond a transition period in which "legacy equipments which do not support key recovery"—that is, key escrow—"can be used to communicate with users" of the escrowed PKI.[168] Apparently, although the report never says so in so many words, the Interagency Working Group believes that after the transition period is over nonescrowed keys will be excluded from the PKI, and the PKI will be designed so that cryptographic products that do not require escrow are prevented from communicating with it.

Exactly how this might be achieved is not explained. One possibility is that the Administration might seek legislation imposing licensing requirements for CAs that require key escrow. The Interagency Working Group states that "Certificate authorities will operate within performance standards set by law"[169] and that "CAs must meet minimum standards for security, per-

---

[165] See note 111 and accompanying text.

[166] See *CRISIS Report* at 6-9 (cited in note 1).

[167] *White Paper* at 3 (cited in note 138).

[168] Id.

[169] Id at 4.

formance, and liability. A Policy Approving Authority (PAA) certifies CAs for operation. *The PAA sets rules and responsibilities for . . . setting CA performance criteria to meet law enforcement needs.*"[170] This statement could mean that escrow-equipped CAs will have to demonstrate they are ready, willing, and able to provide keys or key fragments, when required to do so. Or, it might mean something more, for example that the PAA will not certify CAs that refuse to escrow their subscribers' private keys and that these CAs will be ineligible for whatever liability safe harbor the rules offer. A third possibility is that CAs that refuse to escrow keys will not be allowed to operate at all. This last version sits oddly with the idea of voluntary participation in the PKI. Even if the PAA is benign, its ability to prescribe policies, and the consequences for CAs of noncompliance, would give the PAA the ability to implement restrictive requirements if a new administration were to decide upon a more restrictive policy.[171]

The most perplexing statement in the *White Paper* may be that "Products that operate with an escrowed [public key-management infrastructure] need to be developed with industry taking the lead."[172] Industry is already "taking the lead" in developing a national key management infrastructure without key escrow.[173] The Interagency Working Group apparently hopes that it can change this behavior by allowing escrowed products with strong encryption to be exported; if that fails, the threat in reserve is that the national PKI will not communicate with products that do not escrow keys. Neither of these inducements appears sufficiently powerful to produce much of a groundswell for escrow in the face of customer resistance. Export controls matter less to the utility of a PKI than to cryptosystems in general, since the certificates can be freely exported even if the software that produces them cannot. Admittedly, foreign users will not be able to check the validity of a certificate unless they are able to secure a foreign supply of compatible encryption software or hardware. This possibility, however, seems increasingly likely, and means that even foreign users will be able to use U.S. certificates (or that U.S. users will end up buying a foreign product). The domestic market may in any case become large enough to support a

---

[170] Id at 6 (emphasis added).

[171] See *CRISIS Report* at 329 (cited in note 1) (noting fears of critics of escrow that future administrations may change policy).

[172] *White Paper* at 3 (cited in note 138).

[173] See, for example, *Verisign Homepage*, http://www.verisign.com.

large, unescrowed PKI. Similarly, the absence of a government root certificate may be of only marginal consequence so long as nonmembers of the escrowed PKI are otherwise able to compete on a level playing field with CAs that escrow. The domestic market appears capable of growing its own public-key infrastructure—indeed, several competing ones—without a government-approved authority to supply a root certificate. Netscape, for example, includes a certificate option in version 3.0 of its browser software and allows the user to select which of several types of certificates she wishes to accept.[174] So long as the government does not require them to conform to its policies, private CAs may not care whether they are excluded from the official PKI. On the other hand, if only licensed, escrow-compliant CAs benefit from safe harbors from liability, noncompliant CAs may face significant competitive disadvantages.

The *White Paper* contemplates a federal role in designing a national public-key infrastructure. Several states, including Utah, Washington, Florida, and California, have already passed digital signature legislation of varying degrees of precision, and other states are considering following suit.[175] The Utah and Washington acts provide safe harbors from liability for CAs that comply with relatively strict rules regarding bonding, auditing, and performance; CAs that do not comply are left to the tender mercies of the common law.[176] The Interagency Working Group proposes national legislation "establishing liability protection for certificate authorities who exercise due prudence in the fulfillment of their performance obligations,"[177] but its report does not address the federalism issue. If, however, it becomes federal policy to disadvantage CAs that are insufficiently attentive towards the federal interest in key escrow, the federal law may need to preempt existing and anticipated state efforts to create a

---

[174] The current list offers users a choice among certificates issued by BNN, the U.S. Postal Service, VeriSign, Keywitness, Thawte Server, MCI Mall, Canada Post Corporation, GTE CyberTrust, AT&T Directory Services, and CommerceNET.

[175] See, for example, Utah Code Ann § 46-3-103 et seq (1996). As of November 1995, no certification authorities had qualified under the Utah Act. See Introductory Commentary, History and Current Status of the Utah Act § 1, available online at http://www.state.ut.us/ccjj/digsig/dsut-int.htm. The state of California has passed a statute delegating to the Secretary of State powers to make rules regulating the use and verification of digital signatures. See 1995 Cal Legis Serv Ch 594, AB 1577, 1995-96 Reg Sess ch 594, 3584-85 (West). On March 29, 1996, Washington State approved a digital-signatures statute with an effective date of January 1, 1998. See Washington Electronic Authentication Act, 1996 Wash Legis Serv SB 6423, 1996 Reg Sess ch 250 (West).

[176] See generally Froomkin, 75 Or L Rev 49 (cited in note 64).

[177] *White Paper* at 10 (cited in note 138).

hospitable legal climate for CAs. Whether or not it preempts state law, national legislation might encourage standardization among CAs' policies, which could tend to have a healthy effect on electronic commerce.[178]

Any PKI-based escrow scheme would require federal legislation to determine a number of issues, including:

- the extent of a Title III exemption for escrow agents;
- liability rules for escrow agents; and
- the establishment of the PAA as a federal agency.

Indeed, the Interagency Working Group acknowledges that legislation may be needed to ensure that if an organization acts as its own escrow agent, the person holding the keys is prohibited from tipping off a target that it is the subject of an investigation.[179] The draft report also notes that legislation should criminalize the unauthorized disclosure or use of an escrowed key and create a civil remedy for an aggrieved keyholder.

C. Possible Moves Towards Global Escrow

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.[180] As it becomes increasingly likely that the ITAR will be relaxed, or possibly even eliminated,[181] foreign governments may feel increased pressure to grapple with the cryptography issue.[182] Al-

---

[178] See Froomkin, 75 Or L Rev 49 (cited in note 64).

[179] *White Paper* at 9 (cited in note 138).

[180] Export controls have never been sufficiently well-policed to prevent individuals from carrying out software on disks or computers, or from e-mailing software across borders on the Internet. But, unless one is personally able to check the validity and implementation of an algorithm, one must take cryptographic software on trust. Most firms find it easier to trust something that comes in a box with a famous tradename on it than something illegally exported via the Internet. See Froomkin, 75 Or L Rev at 54 nn 20-21 (cited in note 64).

[181] See note 33 and accompanying text (discussing *Bernstein* decision).

[182] See Stewart A. Baker, *Summary Report on the OECD Ad Hoc Meeting of Experts on Cryptography*, http://www.us.net/~steptoe/276908.htm (1996). A survey of foreign laws

ternately, 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.

Foreign governments have expressed interest in controlling the use of strong cryptography within their borders. France "has the most comprehensive cryptologic control and use regime in Europe, and possibly worldwide,"[183] although these laws are generally not enforced.[184] France recently passed legislation to relax its currently strict control on the domestic use of encryption products—but only if a key to the product is escrowed in France with one of a small number of escrow agents certified by the French government.[185] Russia has not yet embraced escrow, but Russian President Boris Yeltsin issued a decree banning unauthorized encryption.[186] The edict bans the development, import, sale, and use of unlicensed encryption devices, as well as "protected technological means of storage, processing and transmission of information."[187]

In contrast, the current UK policy statement begins with the promise that it "is not the intention of the Government to regulate the private use of encryption"[188] although it goes on to describe a system of licensing and regulation for trusted third parties so as to "engender trust" in them while balancing "the commercial requirement for robust encryption services," the need to protect users, and the need of "intelligence and law enforcement

---

relating to encryption can be found at Bert-Jaap Koops, *Crypto Law Survey*, http://cwis.kub.nl/~frw/people/koops/lawsurvey.htm (1996). Foreign laws on the exportation of cryptographic software are surveyed in *Export Study* (cited in note 9).

[183] *Export Study* at II-17 (cited in note 9).

[184] *CRISIS Report* at 436 (cited in note 1).

[185] See *La loi sur les télecoms met l'Internet en laisse*, bulletin lambda 2.08 (June 10, 1996) (available online at http://www.freenix.fr/netizen/208.html) (describing Article 12 of new telecommunications law and noting passage of legislation in the dead of night); Jerome Thorel, *As French Hang a Leash on the Net, Military Interests Surface*, http://www.tis.com/crypto/cke/press/french.txt (June 14, 1996); Steptoe & Johnson, *Proposed Statutory Trusted Third Party Rules for Encryption*, http://www.us.net/~steptoe/france.htm (analyzing proposed version of law).

[186] *Edict of the President of the Russian Federation On Measures to Observe the Law in Development, Production, Sale and Use of Encrypting Information*, http://www.us.net/~steptoe/edict.htm (Apr 3, 1995).

[187] Steptoe & Johnson, *Russian Statutes Restricting Use of Encryption Technologies*, http://www.us.net/~steptoe/cyber.htm (1996) (quoting *Edict* cited in note 186).

[188] UK Department of Trade and Industry, *Paper On Regulatory Intent Concerning Use Of Encryption On Public Networks* ¶ 8, http://www.coi.gov.uk/coi/depts/GTI/coi9303b.ok (June 10, 1996)

authorities to retain the effectiveness of warranted interception."[189] Japanese policy appears to be moving even further in the direction of decontrol. Former NSA General Counsel Stewart Baker describes a market-driven "emerging Japanese consensus" that encryption is a major technology essential to "Japan's penetration of the Global Information Infrastructure" and warns that unless Japanese policy alters as a result of participation in international policy discussions it "could pose a major challenge" to U.S. escrow policy.[190]

At the international level, the European Union ("EU") has proposed a project to establish a European network of trusted third parties under the control of member nations that seems to resemble the UK proposal. In the EU scheme users may choose to deposit their keys with trusted third parties, in which case the keys are subject to subpoena, but the EU proposal does not suggest that escrow should be mandatory.[191] In 1995 the Council of Europe resolved that member nations' criminal procedure laws should be "reviewed with a view to making possible the interception of telecommunications and the collection of traffic data in the investigation of serious offenses against the confidentiality, integrity and availability of telecommunications or computer systems."[192] The same resolution also advised that "[m]easures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting its legitimate use more than is strictly necessary."[193] Where the line should be drawn, and whether governments should do more than "consider" the measures, the resolution does not say.

The Organization for Economic Cooperation and Development ("OECD") intends to negotiate multilateral cryptography guidelines by the end of 1996.[194] OECD deliberations are not open to the public, and there appears to be no public information about the likely shape of the guidelines. The OECD did, however, hold public meetings with outside experts in Canberra, Paris,

---

[189] Id ¶¶ 5, 7.

[190] Stewart A. Baker, *Emerging Japanese Encryption Policy*, http://www.us.net/~steptoe/276915.htm (1996).

[191] See Denning, *Comments on the NRC Cryptography Report* (cited in note 134) (describing as-yet-unpublished EU proposals).

[192] *Concerning Problems of Criminal Procedure Law Connected with Information Technology*, Council of Europe Recommendation No R (95) 13 at Appendix ¶ 8, (Sept 11, 1995) (available online at http://www.privacy.org/pi/intl_orgs/coe/info_tech_1995.html).

[193] Id at Appendix ¶ 14.

[194] *White Paper* at 8 (cited in note 138).

and Washington, D.C. Some participants in those meetings report that the OECD seems to be considering an escrow-based system,[195] but another says that the governments did not appear to be in agreement: Scandinavian countries were "prominent among the doubters," and "Japan also showed little interest in controlling encryption."[196] The official U.S. government position is that "We are encouraged . . . by recent discussions we have had at the Organization for Economic Cooperation and Development (OECD) that are leading to international cryptography management principles which support [key escrow]."[197]

Whatever it decides, the OECD resolution is likely to be influential. If the OECD member nations were to unite in favor of escrow, it would greatly aid the U.S. government's attempt to make key escrow the norm. The lack of reliable information about the OECD proceedings highlights a key point about the OECD as a forum for deciding social policy. It is not a democratic organization. The executive branch of the U.S. government selects the U.S. delegation; the U.S. delegation will presumably reflect existing U.S. policy. The executive branch is committed to escrow, although there is little evidence that Congress has a considered view of the issue. Nor is there much evidence that the issue has popular salience, although the U.S. escrow policy has a small and, it seems, growing band of opponents drawn from the software industry and the civil liberties lobby. As a result, the

---

[195] See *CRISIS Report* at 448-49 (cited in note 1) (stating that a "number of participants" favored trusted-third-party approach to escrow, although needs of national security "were not mentioned for the most part"). Steve Walker, the founder of Trusted Information Systems, a leading supplier of escrowed encryption systems, reported that,

> The consensus of the [December 1995 Paris] meeting was that user-controlled key escrow provides the only workable solution to the long-standing dilemma between the private sector's need for encryption protection and governments' needs to be able to decrypt the communications of criminals, terrorists, and other adversaries. Other meetings will follow, but it appears that most major governments endorse the U.S. government's user-controlled key escrow initiative as the only practical way through the cryptography maze.

TIS—Building in Big Brother for a Better Tomorrow, http://infinity.nus.sg/cypherpunks/dir.archive-96.02.22-96.02.28/0114.html (e-mail from Steve Walker, Feb 2, 1996, quoted in e-mail from John Young, Feb 22, 1996, to cypherpunks@toad.com).

[196] Stewart A. Baker, *Summary Report on the OECD Ad Hoc Meeting of Experts on Cryptography*, http://www.us.net/~steptoe/276908.htm (1996).

[197] *US Cryptography Policy: Why We Are Taking the Current Approach* (cited in note 107).

executive branch is selling, and helping to shape, an international policy that does not have wide support at home.

The OECD has no legislative power of its own. Any OECD resolution would need to be implemented by appropriate U.S. legislation or regulation. The ITAR (to the extent that they are constitutional) derive from valid statutes, but neither Clipper, software key escrow, nor the *White Paper* approach have been approved or authorized by Congress. It is unlikely to have escaped U.S. policy makers that one way to sell escrow to a potentially skeptical Congress is to present it as the considered fruit of an international consensus against a common threat of lawlessness or terrorism. Those who believe the escrow policy is right are likely to call this statecraft; those who disagree would probably use a different term.

IV. THE TRUST DEFICIT

The struggle over encryption policy is bound up in hopes and fears. The government warns of projected crime waves and feared losses to intelligence gathering. Neither, so far as one can tell, has yet to come to pass. Nevertheless the Administration apparently considers the risk sufficiently great to justify complex maneuvers to shape the development of a nascent industry. Meanwhile, would-be producers and exporters of cryptographic products forecast immense sales, and suggest that cryptography will be built in to any important commercial or social activity that involves a computer. To date, however, the dollar value of cryptographic sales remains fairly low. For their part, cyber-savvy civil libertarians suggest that encryption is a tool that, deployed sufficiently widely, can protect citizens against unwarranted government and corporate intrusions into personal lives. So far, however, a sufficiently large critical mass of users has yet to appear. Thus, each of these perspectives involves an extrapolation. Each vision projects a future in which different hopes or fears predominate. Each vision, however, shares a common supposition that cryptography's importance to society will increase dramatically.

The "widespread [nongovernment] use of cryptography in the United States and abroad is inevitable in the long run."[198] The

---

[198] National Research Council, Kenneth Dam and Herb Lin, eds, *Cryptography's Role in Securing the Information Society* 4-6 (National Academy Press, 1996) (*"CRISIS Report"*) (cited in note 1).

Chairman of the National Research Council's cryptography-policy study committee, Kenneth Dam, is surely correct when he describes the response to this reality as being more a policy crisis than a technology crisis.[199] As the committee stated,

> National cryptography policy should be developed by the executive and legislative branches on the basis of open public discussion and governed by the rule of law. Only a national discussion of the issues involved in national cryptography policy can result in the broadly acceptable social consensus that is necessary for any policy in this area to succeed. A consensus derived from such deliberations, backed by explicit legislation when necessary, will lead to greater degrees of public acceptance and trust, a more certain planning environment, and better connections between policy makers and the private sector on which the nation's economy and social fabric rest.[200]

This is a tall assignment. The key-escrow debate is a particularly acute product of a trust deficit that is national in scope and extends far beyond cryptography. Secrets are most appealing when trust is lacking. Rational citizens concerned about state intrusions into their privacy will be more likely to clamor for the type of protection that cryptography offers as their trust in the state decreases. In a democratic society where many citizens' trust in government and other institutions has been badly bruised, if not shattered,[201] only the most democratic, straightforward, and open process of policy formation could hope to persuade people that the government deserves to have the means to hear every conversation and read every document—even when the government requires legal process to do so. The number of lawful wiretaps is increasing annually,[202] and one can expect even more rapid increases if computer-aided speech and voice

---

[199] Id at xiii.

[200] Id at 8-10.

[201] See A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U Penn L Rev 709, 732-34 (1995) (cited in note 7) (discussing abuses by law enforcement and intelligence agencies); Richard Morin & Dan Balz, *Americans Losing Trust in Each Other and Institutions; Suspicion of Strangers Breeds Widespread Cynicism*, Wash Post A1 (Jan 28, 1996) (describing poll showing that U.S. citizens have profound lack of trust in government and other institutions).

[202] See Jim McGee, *Wiretapping Rises Sharply Under Clinton*, Wash Post A1 (July 7, 1996).

print recognition improve to the point that expensive human interventions can be decreased.[203]

The more that citizens feel they cannot trust the state, the more reason the state may have to fear its citizens. The more that the state fears its citizens, the more citizens may come to believe that they have something to fear from the state. Perceptions can become as important as realities. The state may seek expansive surveillance capabilities because it is sincerely concerned about a foreign threat, or about domestic terrorism. Once citizens engage in "threat analysis" of their government, however, they may see themselves as possible targets of surveillance.

The Administration's hopes of persuading the nation that the government should be trusted with the means of acquiring the people's secrets have been undermined by differences in opinion within the Administration. As a result, the Administration has been unable to speak with one voice. For example, soon after the White House announced that the Administration had no plans to restrict the use of cryptography within the U.S., FBI Director Freeh commented that "[i]f five years from now . . . what we are hearing is all encrypted material that the FBI is unable to decipher, then the policy of relying on voluntary compliance with [escrowed encryption] will have to change."[204]

The Administration has also been hampered by the inconsistency and lack of clarity that characterize its proposals. First the Administration seeks to manipulate markets to achieve its objects. Then it celebrates the role of "industry taking the lead" in developing escrowed products. Then it proposes a new agency, a PAA,[205] with a vague mandate to regulate an important segment of industry. Meanwhile, agencies such as NIST and the Interagency Working Group organize elaborate consultation processes, solicit input from affected industries and the public, and then ignore most of what is said.

One can wonder whether any process of policy formation could be equal to the challenge of persuading *fin de siècle* America to trust the government with its secrets. So far the process has certainly not been up to the job. Instead of being part of a carefully framed national cryptography policy, Clipper, software key escrow, and the *White Paper* represent hastily designed, if

---

[203] See Froomkin, 143 U Penn L Rev at 806 (cited in note 7).

[204] Louis Freeh, *Keynote Luncheon Address at the International Cryptography Institute* (Sept 23, 1994) (excerpt on file with the *Legal Forum*).

[205] See note 172.

nonetheless technically and bureaucratically elegant, stopgaps in the face of a worldwide cryptographic upheaval. Although the Administration's actions have remained carefully within the letter of the law, its tactics have been too manipulative to have any hope of seeming legitimate. Clipper sought to use government standard-setting and buying power to rig the encryption market. Software key escrow sought to hitch escrow to business's need for data security. Now, the *White Paper* proposes that escrow be built into the sinews of electronic commerce.

Clipper was rejected, and software key escrow is unlikely to have a major effect on the market even if it is not abandoned. It is too soon to tell what will happen to the attempt to build escrow into the PKI proposed by the *White Paper*, but the number of unanswered questions, and the inherent tension between the *White Paper's* emphasis on control and its emphasis on market solutions, suggest this policy too will either evolve or die (or both). Whether any of these policies would be publicly acceptable is perhaps open to debate; none deserves to win public acceptance without a Congressional imprimatur.

The past few years have seen cryptographic policy being formed in a semi-open manner. Policies have been developed in secrecy and without consultation,[206] but they have then been announced openly before they went into effect. Public meetings have been held to discuss them—even if afterwards it was often unclear whether the meetings had any significant effect on the results. Information about the government's plans may not have sufficed to cure the trust deficit, but it did allow those opposed to the Administration's proposals to learn what they were and thus to organize their response. In this sense, the move to policy formation at the international level just when the national policy is being contested risks being a retrograde and undemocratic step.

The Administration's concession in the *White Paper* that legislation will be needed to establish a domestic cryptography-control policy represents a quiet turning point in the U.S. cryptography debate, and may provide the means of defusing the crisis. Until now the Administration has worked hard to keep Congress out of the policy loop. Clipper was designed to be formally voluntary and to work through market manipulation. It could be implemented without any legislation. Software key escrow required at most technical legislation to regularize the

---

[206] See *CRISIS Report* at 188 (cited in note 1) (noting comments of relevant stakeholders who felt that policies were "sprung" on them).

rights and duties of private escrow agents. Most of the policy could be implemented administratively, by issuing a FIPS and by modifying the administration of the ITAR. Again, the Congressional role was minimized.

The *White Paper* proposes policies that cannot be implemented without Congressional approval. It does so at a time when Congress seems, for the first time, to be focusing serious attention on the cryptography policy debate although no consensus has yet emerged. Some legislators have proposed bills that would decontrol cryptography[207]; others suggest imposing domestic cryptography controls.[208] The publication of the National Cryptography Study not only removes an excuse for further Congressional delay, but provides middle-of-the-road proposals around which at least a temporary compromise might be fashioned.[209]

The entry of Congress into the field of debate is surely a healthy development. Its participation should add democratic legitimacy to whatever policy is decided, a legitimacy that the executive's creations could never attain alone. That said, it is difficult to be sanguine about the chances that Congress will add much to the quality of the policy being formed. Congress's track record in this area is far from stellar, both on substantive and procedural grounds. The Digital Telephony Act, which requires that all telephone switching networks be made wiretap-friendly if the government pays for the modifications, was rushed through both houses of Congress with next to no debate shortly before the end of the 1994 legislative session.[210] The next Congress, however, balked at appropriating the half a billion or more dollars it

---

[207] See Encrypted Communications Privacy Act of 1996, S 1587, 104th Congress, 2nd Sess (1996); Promotion Of Commerce On-line In The Digital Era (PRO-CODE) Act Of 1996, S 1726 (1996); Security and Freedom Through Encryption (SAFE) Act, H R 3011 (1996).

[208] Senator Grassley introduced the Anti-Electronic Racketeering Act (June 27, 1995), which would prohibit distribution of unescrowed computer software "that encodes or encrypts electronic or digital communications to computer networks that the person distributing the software knows or reasonably should know, is [sic] accessible" to foreigners. For a discussion of the highly debatable constitutionality of a domestic ban on unescrowed cryptography, see Froomkin, 143 U Penn L Rev at 810-43 (cited in note 7).

[209] The Report was attacked in surprisingly gentle terms by both partisans of escrow and partisans of complete decontrol. Compare note 134 and accompanying text with note 135 and accompanying text.

[210] 47 USC § 1001 et seq (1994). See 140 Cong Rec S14666 (Oct 7, 1994) (reporting the Senate's passage of the bill by voice vote); 140 Cong Rec H10917 (Oct 5, 1994) (reporting the House's passage of the bill by two-thirds vote).

would have taken to implement the retrofitting required by the act.

The publication of the National Research Council's report, *Cryptography's Role in Securing the Information Society*, is the most encouraging development in the cryptography debate. The report emphasizes that national security is enhanced by the widespread use of encryption to secure personal and corporate data and to protect computer-controlled operations, such as electricity generation and power supplies. The report makes clear that these gains deserve to be weighed in the balance. Because widespread cryptography is inevitable, the only loss to U.S. law enforcement and intelligence-gathering capabilities is the short-term, but immediate, loss from abandoning efforts to stem the tide. Given this forecast, the report concludes that the gains from allowing free export of DES outweigh the short term losses suffered above the inevitable long-term losses.[211]

Reasonable people may differ with some of the National Research Council's recommendations,[212] but they form a solid starting point for an informed debate. On July 12, 1996, however, the Administration announced that its fundamental commitment to an escrow policy remained unchanged.[213] The battle over cryptographic key "escrow" is only beginning to heat up.

POSTSCRIPT: THE OCTOBER 1996 "INITIATIVE"

The *White Paper* bore its first fruit in the Clinton Administration's October 1996 cryptographic policy initiative. Although no formal actions had been taken at the time this article went to press—neither executive orders nor proposed or final regulations had been issued—the Administration let it be known

---

[211] *CRISIS Report* (cited in note 1).

[212] Indeed, I cannot resist noting that I strongly disagree with Recommendation 5.4: "Congress should seriously consider legislation that would impose criminal penalties on the use of encrypted communications in interstate commerce with the intent to commit a federal crime." *CRISIS Report* at 332 (cited in note 1). Recommendation 5.4 is notably more tentative than any other in the Report, and deservedly so. The goal of discouraging the use of cryptography for illegitimate purposes is laudable, but the proposed statute is a bad idea, badly thought out. There is no evidence that such a statute would deter the use of cryptography in a world in which cryptography is seamlessly included in most e-mail and telecommunications. While it is unclear what the effects of such a statute would be once cryptographic tools become ubiquitous and invisible, the odds are that every federal crime involving a communication would also violate the statute. The two federal crimes would then be predicate RICO offenses, and so on . . . .

[213] See *Administration Statement on Commercial Encryption Policy*, http://csrc.ncsl.nist.gov/keyescrow/admin.txt (July 12, 1996).

that it planned to implement the new policy by executive order in early 1997.

The October policy initiative had two major parts. First, the Administration proposed to transfer primary jurisdiction over cryptographic control from the U.S. Munitions List administered by the traditionally more cautious State Department to the Commerce Control List, administered by the traditionally more export-oriented Commerce Department.[214] Second, the Administration proposed to allow temporary export of fifty-six-bit encryption products—i.e. of DES, the de facto global standard commercial encryption product—but for no more than two years, and only so long as the exporters promised "to build and market future products that support key recovery[215]," albeit with an option to have keys held by approved private parties rather than the government.[216] Grants of export permission would be for six months at a time, and would be contingent on "commitments from exporters to explicit benchmarks and milestones for developing and incorporating key recovery features into their products and services, and for building the supporting infrastructure internationally."[217] In other words, companies that promise to build key escrow products (for domestic use as well as international?) will be allowed to export DES, but others will not. And all exporters will be on a short leash to ensure continued compliance.

A rigorous analysis of the revised policy is impossible before the implementing regulations are issued, but some initial points stand out. By allowing the virtually unlimited export of DES products via the CCL list, the Administration would effectively

---

[214] On the "subtle but nonetheless significant" effects of this change see Stewart A. Baker & Peter Lichtenbaum, *Cutting the Red Tape on Encryption*, The Journal of Commerce 9A (Sept 27, 1996). For a description of the mechanics of the administration of the two lists, see Ira S. Rubinstein, *Export Controls on Encryption Software*, in *Coping with U.S. Export Controls 1994* at 401 (PLI Com Law & Practice Course Handbook Series No A-705, 1994).

[215] By using the term "key recovery" rather than "key escrow," the Administration means to signal its acceptance of an alternate means of preserving its potential access to keys. In a "key recovery" system, the user's private key is not stored with the escrow agent. Instead, every message contains a LEAF-like structure which has the message's session key encrypted with a public key belonging either to the escrow agent or to law enforcement. Possession of the matching key still gives full access to all messages sent by the user using the system, but it improves over the original Clipper proposal in that this access does not provide the technical capability of forging a message that appears to originate from the user.

[216] White House, Office of the Vice-President, *Statement of the Vice President, Oct 1, 1996*, http://www.cdt.org/crypto/clipper311/961001_Gore_stmnt.html.

[217] Id.

concede that additional exports of DES are not, in and of themselves, a serious incremental threat to the national security. In addition, by limiting export permission to firms that prove they are on board and contributing to the Administration's desire for an escrow-enabled infrastructure, the policy also concedes the bankruptcy of the claim that industry spontaneously is "taking the lead"[218] in developing escrowed products in response to consumer demand.

The proposal to ration export licenses according to the business plans or practices of applicants is especially troubling. Ordinarily (although, as discussed below, not at this moment), the federal authority to control exports arises from two statutes, the Export Administration Act[219] and the Arms Export Control Act.[220] Neither of these statutes was intended to give the executive branch the authority to direct the industrial policy of the United States, and neither act has ever been understood by anyone involved in export control as giving the government that power.[221] The government might argue that national security would in fact be improved by accelerating the development of strong escrowed products. Or, more subtly, the government might even argue that *only* the acceleration of development can mitigate the harm caused by exports of DES products, on the theory that foreign consumers will migrate to the stronger albeit escrowed products, leaving the unescrowed DES products as a transitional nuisance. Even if one were to embrace these arguments, however, it in no way follows that either the EAA or the AECA gives the government the authority to implement a preferential export policy by which one's right to export one product depends on one's plans to develop another. These are export control statutes, not a blank check to conduct industrial policy.[222]

A further aspect of the initiative is also disturbing. The EAA expired in August 1994. President Clinton immediately declared a national emergency and issued Executive Order 12924 extend-

---

[218] See notes 172 and 205 and accompanying text.

[219] See note 20.

[220] See note 19.

[221] A would-be exporter denied permission to export a DES-based product would seem to have a fairly strong case that the refusal to grant a license under the EAA was arbitrary and capricious, and therefore contrary to the Administrative Procedure Act. Unfortunately for the would-be exporter, decisions under the EAA are not subject to judicial review under the APA. See EAA, 50 USC App § 2412(a) (1988 & Supp V 1993).

[222] Compare *Industrial Union Department v American Petroleum Instststitute*, 448 US 607, 644 (1980) (refusing to find that Congress delegated "unprecedented power over American industry" in the absence of a "clear mandate" in OSHA statute).

ing the EAA "[t]o the extent permitted by law."[223] The only authorities noted in Executive Order 12924 are the President's inherent constitutional authority and the International Emergency Economic Powers Act ("IEEPA").[224] Assuming that the President does not have inherent constitutional authority to block exports in peacetime, the authority for this action is IEEPA, which by its own terms applies to "any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States . . . if the President declares a national emergency with respect to such threat."[225] While Executive Order 12924 refers to the danger of "unrestricted access of foreign parties to U.S. goods, technology and technical data," it seems that the real "unusual and extraordinary" threat consists of Congress's failure to renew the EAA. Indeed, the President's most recent renewal of the state of emergency admits that the state of emergency must be extended "[b]ecause the Export Administration Act has not been renewed by the Congress."[226]

While this is far from the first time that the EAA export control regime has been continued by executive order after a lapse in statutory authority,[227] there is nevertheless something unsavory about a state of emergency being used for more than a very short time to cover a Congressional refusal to reenact a statute. An emergency of this sort that lasts more than one Congress is suspect indeed. Others have suggested that IEEPA should be amended to prevent the existence of "perpetual emergencies,"[228] and as it wears on they may find in this "emergency" more evidence of the need for a reform.

---

[223] Continuation of Export Control Regulations, Exec Order No 12924, 59 Fed Reg 43437 (1994). See also Continuation of Emergency Regarding Export Control Regulations, 61 Fed Reg 42527 (August 14, 1996).

[224] 50 USC § 1702 (1988 and Supp IV 1992).

[225] IEEPA, § 202(a), 50 USC § 1701 (1988 and Supp IV 1992).

[226] Continuation of Emergency Regarding Export Control Regulations, 61 Fed Reg 42527 (Aug 14, 1996).

[227] The predecessor version of the EAA expired in September 1990 and was continued in effect by President Bush, see Exec Order No 12730 (1990), 55 Fed Reg 40373 (Sept 30, 1990). Similarly, President Reagan kept the CCL regulations in force for more than a year, from Exec Order No 12470 (March 30, 1984) until the repassage of the EAA in Pub Law 99-64 (July 12, 1985). See Exec Order No 12525, 50 Fed Reg 28757 (July 12, 1985). Exec Order No 12444, Oct 14, 1983, 48 Fed Reg 48215, which had provided for the continued effectiveness of the Export Administration Act of 1979, was revoked by Exec Order No 12451, Dec 20, 1983, 48 Fed Reg 56563.

[228] See, for example, Harold Hongju Koh, *The National Security Constitution* 197 (Yale University Press, 1990).

Given, however, that IEEPA provides the current authority for the continuance of the EAA regime, and that the Clinton Administration proposes to move DES, however temporarily, off the USML and onto the CCL, a creation of the EAA,[229] it seems reasonable to ask to what extent IEEPA authorizes the October Initiative and to what extent parties aggrieved by the new regulations will be able to challenge them. Several challenges seem possible. Indeed, as set out in more detail below, there is a strong argument that IEEPA does not give the government the authority to control the export of cryptographic software once it has been removed from the USML. Since the October Initiative involves moving DES from the USML to the CCL, this may have the unintentional result of allowing unlimited export of DES-based software.

First, while its terms are indeed sweeping, IEEPA is no more a grant of the power to conduct industrial policy than is the EAA. Second, IEEPA lacks the prohibition on judicial review in the EAA. License denials premised on IEEPA can thus be challenged under the APA, even if the IEEPA authority is being used to extend the rules originally developed under the more restrictive review provisions of the EAA.[230] It might even be possible to argue in the context of an IEEPA challenge that the extension of the EAA licensing regime contemplated in the October Initiative exceeds the powers granted in the EAA—even though that claim would be difficult, albeit not impossible,[231] to bring under the EAA itself.

Third, it may be significant that IEEPA imposes in 50 USC section 1702 a limit on the President's authority, one designed to protect the free flow of ideas:

> The authority granted to the President by [the part of IEEPA that grants sweeping power to control exports during a national emergency] does not include the authority to regulate or prohibit, directly or indirectly . . . the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials,

---

[229] See note 214 and accompanying text.

[230] See John Ellicott, et al, *Judicial Review Under Export Laws* in Evan R. Berlack and Cecil Hunt, eds, *Coping with U.S. Export Controls* 1994 at 353, 371 (PLI Commercial Law and Practice Series A-705, 1994).

[231] See id at 362-67; *Bozarov v United States*, 974 F2d 1037 (9th Cir 1992); *Dart v United States*, 848 F2d 217 (DC Cir 1988).

> including but not limited to microfiche, tapes, compact disks, CD ROMs, artworks and news wire feeds.[232]

In turn, this restriction on the President's sweeping authority to control exports under IEEPA is itself subject to an exception: "The exports exempted from regulation or prohibition by this paragraph do not include those which are otherwise controlled for export under section 5 of the Export Administration Act of 1979,[233] or under section 6 of such Act,[234] to the extent that such controls promote the nonproliferation or antiterrorism policies of the United States . . . ."[235]

There are two ways one might read this. On the one hand, IEEPA's reference to the EAA could be an incorporation by reference. In this reading, the President's IEEPA powers are unaffected by subsequent changes in the EAA. Indeed, it matters not whether the EAA is amended or expires—whatever powers were contained in the EAA when the relevant portion of IEEPA was last enacted[236] remain reserved to the President. This reading is buttressed by the so-called "Lazarus Rule"[237] under which specific references to a statute survive that statute's repeal.[238] Any other rule, the Supreme Court explained in *Kendall v. United States*, would create uncertainty "as to what was the law; and would be adopting prospectively, all changes that might be made in the law."[239]

Alternately, IEEPA's reference to the EAA could be understood as a Congressional decision that its protection of the free flow of ideas is not intended to disrupt the export controls scheme "otherwise" authorized by the EAA, and that if there is no such scheme then there is no IEEPA exception either. In this reading, if the EAA were amended to increase the government's authority to impose export controls, the President's IEEPA authority would automatically increase as well. On the other hand,

---

[232] 50 USC § 1702(b) (1988 and Supp IV 1992).

[233] Codified at 50 USC App § 2404 (1988 and Supp IV 1992).

[234] Codified at 50 USC App § 2406 (1988 and Supp IV 1992).

[235] 50 USC § 1702(b)(3) (1988 and Supp IV 1992).

[236] As it happens, the most recent amendment of 50 USC § 1702(b)(3) occurred on April 30, 1994. See Pub L 03-226, Title V, Part A, § 525(c)(1), 108 Stat 474.

[237] See Note, *"Lazarus Come Forth. And He that Was Dead Came Forth." An Examination of the Lazarus Rule: Fischer v. City of Grand Island*, 26 Creighton L Rev 221 (1992).

[238] See, for example, *Kendall v United States*, 37 US (12 Pet) 524, 624-25 (1838). See also Note, 26 Creighton L Rev at 228-29 (cited in note 237) (collecting authorities).

[239] *Kendall*, 37 US (12 Pet) at 624 (1838) (cited in note 238).

if the EAA lapses or is repealed, the President's IEEPA authority shrinks accordingly. While this might seem to lead straight to the evil that the Supreme Court warned against in *Kendall*, it is important to note that the statutes at issue there referred to the laws of *foreign* jurisdictions. When Congress makes reference to its own laws, the justification for the "Lazarus Rule" is considerably reduced because the danger of prospective adoption of rules of unknown content under the control of other sovereigns is eliminated.[240] Furthermore, the dangers of uncertainty and unintended consequences seem tenuous indeed when Congress is amending laws which are well cross-indexed.

Both the word "otherwise" and the structure of IEEPA suggest that the purpose of the limitations in section 1702 was to ensure that the President has no power to restrict the exchange of information and ideas, while leaving intact regulations promulgated pursuant to the EAA. Since the EAA has lapsed by its own terms, the legislative intent behind the EAA, and arguably IEEPA also, might best be effectuated by a finding that IEEPA does not allow the government to restrict the export of "information or informational materials," a term that would probably include DES software,[241] once those come off the USML. There are, however, no cases of which I am aware which address this issue, and it is likely to be the subject of litigation unless and until Congress renews the EAA.

---

[240] See generally Note, 26 Creighton L Rev at 236 (cited in note 238) (arguing that legislative intent should usually control).

[241] Whether a program is "information or informational materials" as opposed to a mere device is debated. One court has held that cryptographic source code is speech. See *Bernstein v United States*, 922 F Supp 1426 (ND Cal 1996). But see *Karn v United States*, 925 F Supp 1 (D DC 1996). The *Karn* decision is currently under appeal to the D.C. Circuit.