

UIC John Marshall Journal of Information Technology & Privacy Law

Volume 17
Issue 3 *Journal of Computer & Information Law*
- Spring 1999

Article 10

Spring 1999

Digital Signatures, the Electronic Economy and the Protection of National Security: Some Distinctions with an Economic Difference, 17 J. Marshall J. Computer & Info. L. 981 (1999)

Raneta Lawson Mack

Follow this and additional works at: <https://repository.law.uic.edu/jitpl>



Part of the [Computer Law Commons](#), [Internet Law Commons](#), [Privacy Law Commons](#), and the [Science and Technology Law Commons](#)

Recommended Citation

Raneta Lawson Mack, Digital Signatures, the Electronic Economy and the Protection of National Security: Some Distinctions with an Economic Difference, 17 J. Marshall J. Computer & Info. L. 981 (1999)

<https://repository.law.uic.edu/jitpl/vol17/iss3/10>

This Article is brought to you for free and open access by UIC Law Open Access Repository. It has been accepted for inclusion in UIC John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of UIC Law Open Access Repository. For more information, please contact repository@jmls.edu.

DIGITAL SIGNATURES, THE ELECTRONIC ECONOMY AND THE PROTECTION OF NATIONAL SECURITY: SOME DISTINCTIONS WITH AN ECONOMIC DIFFERENCE

by RANETA LAWSON MACK†

Costello: What's the guy's name on first base?

Abbott: What's the guy's name on second base.

Costello: I'm not asking you who's on second.

Abbott: Who's on first.

Costello: I don't know.

Abbott: He's on third, we're not talking about him.

Costello: How did I get on third base?

Abbott: You mentioned his name.

Costello: If I mentioned the third baseman's name, who did I say is playing third?

Abbott: No. Who's playing first.

Costello: Stay off of first will you?

Abbott: Well, what do you want me to do?

Costello: Now, what's the guy's name on third base?

Abbott: No. What's on second.

Costello: I'm not asking you who's on second.

Abbott: Who's on first.

Costello: I don't know.

Abbott: He's on third.

Costello: There I go, back on third again.¹

† Professor of Law, Creighton University School of Law.

1. This immortal Abbott and Costello finale, popularly known as the "Who's On First" sketch, plays continuously on video at the Baseball Hall of Fame in Cooperstown, New York. It is estimated that Abbott and Costello performed their trademark sketch at least 10,000 times.

I. INTRODUCTION

Misunderstanding. Confusion. Frustration. The same words that may be used to characterize this classic comedy dialogue might also be aptly applied to the current national debate surrounding encryption and digital signature technology. In typical debate style, the parties have staked out what appear to be competing positions on the issue of encryption and the need to maintain or relax the current controls on the export of encryption technology. What is atypical, however, is that the parties have apparently failed to clearly define the parameters of the relevant technology that is at the center of the debate. For example, the Clinton administration favors and promotes restrictive export controls to curtail the possibility that strong encryption technology developed in the United States will be available to hostile foreign countries, terrorists and others who might use the technology for unlawful purposes. In sharp contrast, software companies and other civil liberties organizations argue for a relaxation and, in some cases, a complete elimination of these same export controls in order to increase online privacy and security, expand commercial uses of the technology, and ultimately enhance the United States' economic stake in the burgeoning Internet economy. While on the surface it appears that these two interests are diametrically (and perhaps irretrievably) opposed, a closer analysis of the underlying technological issues reveals that the sides are, in fact, debating about two different, although related, uses of encryption technology. Moreover, as will be discussed in this article, the applications of encryption technology being debated by each side are distinct enough that one might even characterize the interests promoted by the business community and private citizens as "benign and non-threatening" to the concerns of national security. Why then do these interests continually collide and apparently result in a state of frustration and bureaucratic inertia with respect to policy and legislation in the area of digital signature technology? As this article will explore, the problem is due in part to a combination of misunderstanding and confusion with respect to the relevant technologies and their applications.

To untangle some of the issues involved in the current digital signature/encryption technology debate, this article will first discuss the relevant technologies and their applications in the online environment. This discussion will demonstrate that while digital signature technology utilizes encryption as part of its process, in most instances, its primary purpose is not the confidentiality of a particular Internet transmission, but the ability to authenticate and verify the participants in an online communication. This article will further explore the competing interests involved in the encryption/digital signature debate by analyzing recent case authority and administrative policies that address the government's

ability to regulate encryption, as well as the potential impact on national security if the current encryption export controls are relaxed or removed. Then, current efforts to draft and implement digital signature laws will be examined to demonstrate how potential threats to national security are negligible when dealing with digital signatures in the global Internet economy. Finally, this article will argue that congressional debate and legislation in the areas of digital signatures and encryption can and should draw a distinction between encryption used primarily for purposes of confidentiality and encryption used as part of the digital signature authentication and verification process. Such separate consideration will allow a clearer understanding of the benign nature and purposes of digital signature technology, and will likely serve as a springboard for enacting uniform federal legislation in the area of digital signatures.

II. DIGITAL SIGNATURE TECHNOLOGY

The technology surrounding the creation and use of digital signatures is somewhat complex, but an explanation and understanding of the technology is an essential prerequisite to dissecting the current debate on these issues. This section of the article will provide a concise (and hopefully clear) explanation of the technology and its current application.

The unprecedented growth of the Internet has created tremendous opportunities for businesses and consumers to develop and participate in global electronic commerce transactions or "e-commerce."² Once primarily the domain of academics, the Internet, and more specifically the World Wide Web ("WWW"), is now a global community of networks accessible to anyone who can afford the price of admission: a computer, a modem and an Internet Service Provider ("ISP"). Once on the Internet, users can access information and interact almost instantaneously with others on a local, regional, national and/or international basis. With that kind of extensive access to potential markets literally at one's fingertips, it did not take long for businesses to recognize the enormous potential for profit afforded by this new global networked community. For example, Company X, selling widgets in Omaha, Nebraska, can, with relatively

2. A study by the United States Commerce Department determined that by the end of 1997, 10 million people in the United States and Canada purchased something on the Internet. The study also predicted that e-commerce could surpass \$300 billion for business-to-business transactions by the year 2002. See U.S. Department of Commerce, *The Emerging Digital Economy Report* (visited May 13, 1999) <<http://www.doc.gov/ecommerce/emerging.htm>>. Other examples of the growth of e-commerce include General Electric Company's plans to buy \$5 billion in materials over the Internet in the next two years and Dell Computer's report that between January 1997 and December 1997, its Internet sales increased from \$1 million per day to \$5 million per day. *Id.*

little cost, now market and sell its widgets to a distributor in Brazil. Company X begins this process by establishing an Internet presence, which means that it uses (or more often pays someone else to use) hypertext markup language ("HTML") to create a Website on the WWW. Commercial web sites can run the gamut from simply describing the company and its products to making the company's entire inventory of goods available for immediate purchase by consumers on the Internet.³ If a company chooses to market and sell its wares on the Internet, then a key component to success is the ability to provide consumers with an efficient, secure and trustworthy environment to complete the purchase transaction. Various surveys have indicated that consumer concerns about privacy and security are significant barriers to purchasing products on the Internet.⁴ Consumers fear that credit card or other personal information will not be protected during the online transaction, and might be intercepted while traveling across the network and used for fraudulent purposes. By the same token, companies offering products for sale on the Internet are concerned that they could suffer financial losses as a result of fraudulent transactions or seemingly legitimate transactions that are later repudiated by consumers. Consider two examples:

Company X in Omaha receives an order for 1000 custom made widgets from Company Y in Brazil. The order is placed through Company X's Website. Based upon this order, Company X creates the custom widgets and ships them to Company Y along with an invoice. Upon receipt of the invoice, Company Y refuses the shipment and advises Company X that a hacker infiltrated Company Y's computer system and fraudulently placed the order.

Company Y in Brazil legitimately places an order for 100 custom made widgets from Company X in Omaha through Company X's Website. However, a hacker intercepts Company Y's order and, just for fun, decides to change the order from 100 widgets to 1000 widgets before sending the transmission on to Company X. Once again, Company X creates the 1000 custom widgets and ships them to Company Y, which immediately rejects the extra 900 widgets. Thus, Company X discovers the fraud only after incurring substantial costs in producing the extra 900 widgets.

In both instances, due to fraudulent conduct by third parties, Company X suffers unanticipated losses as a result of creating the unnecessary custom widgets. Given the potential benefits to merchants and

3. Websites that allow customers to purchase goods online are usually quite complex and often utilize sophisticated databases and graphic imaging technology in addition to HTML.

4. See, e.g., *House Commerce Expands Inquiry Into E-Commerce*, 64 Telecommunications Rep. 21 (May 25, 1998) (discussing a survey conducted by Lycos, a web search engine developer, that identified privacy and security as consumers' top two concerns).

consumers associated with the emergence of a global Internet economy, there must be mechanisms in place to ensure that sensitive information is transmitted securely and confidentially. Further, there must be assurances that parties engaging in particular transactions are authorized to do so, and that the information being transmitted over the Internet reaches its destination without being altered in any manner. In other words, using the special terminology of digital signature technology, parties to e-commerce transactions should be certain that their transactions are confidential, authentic (originating from a person or entity authorized to conduct the transaction), and unaltered. Digital signature technology accommodates each of these goals.

Digital signatures are very much like their written counterparts in the sense that they can legally bind specific parties to a particular transaction. In e-commerce transactions, because the parties may be separated by thousands of miles and it may not be possible or practical to physically sign or authenticate documents representing the parties' agreement, they must create and rely upon "virtual" or digital signatures. The first step in creating a digital signature involves the use of cryptography or encryption technology. Cryptography allows users to scramble (encrypt) and unscramble (decrypt) messages to ensure privacy in Internet communications, and is often analogized to a lock and key system. One party uses a key to lock (encrypt) the message and the recipient uses a separate copy of the key to unlock (decrypt) the message. The "virtual" keys used to lock and unlock messages are measured in lengths and expressed in bits. The longer the key length (i.e., the more bits it contains), the more resistant it is to being arbitrarily guessed or "broken" by someone desiring unauthorized access to the message. For example, if Abe uses a key to encrypt a confidential message sent to Betty, Abe must ensure that Betty has a copy of his key so she can unlock (decrypt) the message upon receipt. If Abe's key length is sufficiently long and complex, then only those who have a copy of his key will be able to decipher messages from him. If Abe's key length is short, however, anyone who intercepts the message as it is en route to Betty might be able to "guess" the key by using special software designed to perform a series of computations until it discovers the correct key.⁵ Once Abe's key is discovered, the interceptor is not only able to unscramble Abe's

5. The most common standard for key lengths is the Digital Encryption Standard (DES), which uses a 56-bit key length. Until recently, it was thought that it would take a significant amount of time and computing hardware and software resources to "discover" a key and decrypt a message encrypted with a 56-bit key. However, in July 1998, using a \$250,000 homemade supercomputer, John Gilmore and Paul Kocher broke the 56-bit key in 56 hours. The government had previously asserted that it was simply not possible to design and make a computer capable of cracking DES.

messages, but can also create and encrypt messages that appear to come from Abe.

Implicit in the foregoing discussion is the fact that both the sender and recipient use the same key to encrypt and decrypt messages, and that the sender will make the necessary key available to the intended recipient of the message. This encryption process is known as symmetric cryptography because the keys used to encrypt and decrypt are the same. The one obvious shortcoming with this form of cryptography is that anyone who gains access to the sender's key can encrypt and decrypt messages. Thus, when the sender supplies his key to a recipient, he must trust that the recipient won't use it improperly or allow it to fall into the hands of someone who might use it improperly. Due to the implicit need to trust the actions of the recipient, it is easy to understand why symmetric cryptography is impractical for e-commerce transactions that take place over the Internet where the parties are often interacting for the first time and have not yet established a trusting relationship.

Another type of cryptography known as asymmetric or public key cryptography is more suitable to the typical e-commerce transaction. With public key cryptography, the sender has a private key, which is not revealed to anyone. That private key is uniquely paired to a public key that is made available to recipients. The public and private keys are linked in such a manner that the public key can decrypt only messages encrypted by the private key. The public key may also be used to encrypt messages, which may only be decrypted by the private key. The differences between this system and the symmetric system are that the private key is kept by the sender and cannot be discovered by examining the public key, and the encryption/decryption process must take place between the public and private keys.⁶ This means that recipients with the sender's public key may not use it to communicate with others who hold the public key. Therefore, public key cryptography has two primary benefits. First, it allows confidential communications between senders and recipients. Second, because the private key is owned and kept by one person, public key cryptography also provides a degree of certainty that the confidential communication originated from the holder of the private key. At this point in the discussion, it is important to note that the use of encryption technology to scramble or unscramble the contents of a message is *not* a digital signature. Instead, as explained below, encryption technology is merely a step in the process of creating a digital signature.

6. Although the private and public key are generated randomly and are uniquely paired, they can nevertheless be "cracked" if the key length is short. Thus, the longer the key length, the more difficult it becomes to use special software to discover the unique key pair.

Once the sender of a message selects a document to be digitally signed and transmitted, she must first create a message digest of the document. The document being transmitted is usually converted into a much shorter message called the message digest because the encryption process is time consuming.⁷ Since each original document is unique, when converted to message digest form, each will create a unique "digital fingerprint." Once the message digest is created, the *digest* is then encrypted with the sender's private key. The *encrypted message digest* is the digital signature. This digital signature is then attached to the original document and sent to the recipient.⁸

Upon receipt of the original document with the attached digital signature, the recipient, who already has the sender's public key, will first decrypt the message digest to reveal the unique digital fingerprint. The recipient then takes the original document transmitted by the sender and, using a special software program, converts it to a message digest.⁹ The two message digests (the one transmitted by the sender and the one created by the recipient from the original document) are then compared. If the two message digests are the same, the recipient can be fairly certain that the original document has not been altered in the transmission. Additionally, because the message digest is decrypted using the sender's public key (which is uniquely paired to the sender's private key), the recipient can be reasonably certain that the message originated with the sender. Certainty with respect to the sender's identity can be greatly enhanced if a third party provides some independent assurance that the private/public key pairs are associated with a particular person or entity. Providing this assurance is the anticipated role of certification authorities in the digital signature infrastructure, and will be discussed later in this article. Certification authorities can establish standards to verify the identities of individuals owning private/public key pairs and issue digital certificates confirming that identity and ownership status. Thus, the recipient of a message can rely upon the sender's digital certificate as further verification of the sender's identity, which adds yet another level of authentication to the entire transaction.

As the foregoing discussion has demonstrated, with digital signature technology, the goals for secure and authentic e-commerce transactions have been accomplished. While encryption technology is a critical component in the digital signature process, it is used primarily to attribute

7. The message digest is also sometimes referred to as the "hash result," and is created by running the original document through a one way hash routine to produce a fixed length message digest.

8. In some instances, the original document may also be encrypted for an additional level of confidentiality.

9. Of course, if the original document was also encrypted, it will have to be decrypted prior to converting it to a message digest.

messages to a particular sender, i.e., to verify the sender's identity through the use of the private/public key system. This is an entirely "benign" use of encryption technology, which adds a necessary level of security to legitimate e-commerce transactions and furthers the goal of promoting the growth of the Internet economy. Nevertheless, because this same encryption technology may be used independent of the digital signature process by criminals and terrorists to send confidential encrypted messages across the Internet, the United States government has imposed restrictions in the form of export controls on the use of certain encryption technology. The export controls on encryption products may indeed prevent the expansion of criminal and terrorist communications across the Internet, but they also impede the benign and legitimate use of that same technology as part of the digital signature process, which is a fundamental building block for the growth of e-commerce. The nature of these export restrictions and the debate surrounding government controls on encryption products will be explored in the next section.

III. ENCRYPTION – THE CONTROLS AND THE DEBATE

The Arms Export Control Act ("AECA") and its implementing regulation, the International Traffic in Arms Regulation ("ITAR"), authorize the President of the United States to control the import and export of "defense articles and defense services" by specifically designating such items and placing them on the United States Munitions List ("USML"). Anyone seeking to import or export items identified on the USML must first seek a license from the government. The ITAR identifies "military cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems" as munitions subject to the licensing requirement.¹⁰ Since this definition is sufficiently broad and could cover a number of devices and applications that use cryptography, the regulations also establish a procedure for determining whether a particular item is subject to the import/export restrictions.¹¹

On November 15, 1996, the President of the United States transferred jurisdiction over non-military encryption products and related technology from the Department of State to the Department of Commerce.¹² Non-military encryption products were then placed on the

10. 22 C.F.R. § 121.1 (1999).

11. This process, known as a commodity jurisdiction procedure, allows the Office of Defense Trade Controls (ODTC) to determine if an article or service is covered by the USML.

12. The transfer of jurisdiction was done pursuant to Executive Order 13026 entitled "Administration of Export Controls on Encryption Products." See, Exec. Order No. 13026, 61 Fed. Reg. 58767 (1996).

Commerce Control List ("CCL") and subject to the Export Administration Regulations ("EAR"), while encryption products for military applications remained on the USML and continued to be regulated by the ITAR. In the Executive Order transferring jurisdiction, the President stressed that "the export of encryption software . . . must be controlled because of [the] software's functional capacity rather than . . . any possible informational value of such software."¹³ The press release accompanying the Executive Order further emphasized that although non-military encryption products were being removed from the USML, these encryption products still had to be controlled for foreign policy and national security interests. If the new regulations proved inadequate for protecting those interests, then the products would be returned to the USML. With certain exceptions, prior to exporting any item on the CCL, a license must be obtained from the Bureau of Export Administration ("BXA"). The BXA reviews all applications on a case-by-case basis to determine whether the export of a particular item comports with national security and foreign policy interests.¹⁴ Encryption software, which is one of the categories regulated by the CCL, is defined as "computer programs that provide capability of encryption functions or confidentiality of information or information systems."¹⁵ This definition includes source code, object code, applications software or systems software. There are a number of exceptions to the licensing requirements, including an exception for certain commercial software items such as mass market encryption software, key recovery software and non-recovery items up to 56-bit key length DES.¹⁶

One of the key definitions in the EAR is the term "export." According to the EAR, export of encryption technology and software means "actual shipment or transmission of items out of the United States."¹⁷ Further, for encryption source code or object code, export includes downloading or causing the downloading of the software to locations outside the United States by making the software available to persons outside the United States through electronic bulletin boards, Internet file transfer protocol ("FTP") and web sites.¹⁸

13. *Id.*

14. The CCL categorizes encryption items according to various criteria including the reason for their control and all items are given an Export Control Classification Number (ECCN).

15. 15 C.F.R. pt. 772 (1999).

16. 15 C.F.R. § 742.15 (1999). These exceptions are available after a one-time review by the BXA. Additionally, items that are already publicly available or contain "de minimus" domestic content are not subject to the EAR. 15 C.F.R. §§ 734.3(b)(3), 734.4 (1999).

17. 15 C.F.R. § 734.2(b)(1) (1999).

18. 15 C.F.R. § 734.2(b)(9).

While the EAR ostensibly focuses on protecting national security and foreign policy interests, one of the major criticisms leveled against the export control regulatory scheme is that it unconstitutionally restricts the availability of information protected by the First Amendment.¹⁹ In *Berstein*, the plaintiff, Daniel Bernstein, a mathematician, sought a declaratory judgment and injunctive relief against enforcement of the export controls, arguing that they were unconstitutional on their face and as applied to the cryptographic computer source code created by Bernstein.²⁰ Bernstein had developed an encryption algorithm known as Snuffle and incorporated the idea for Snuffle into an academic paper and a computer program known as the Snuffle Encryption System. Bernstein submitted both the program and the paper to the State Department for a determination as to whether they would be subject to the export licensing requirements. The Department determined that Snuffle 5.0 was a defense article on the USML and subject to licensing by the government prior to export. The ODTC identified the item as "a stand-alone cryptographic algorithm which is not incorporated into a finished software product."²¹ Bernstein then brought suit alleging that he was not free to teach, publish or discuss his theories on cryptography with other scientists because of the encryption export restrictions. He argued that the export restrictions constituted a prior restraint on his right to free speech, were unconstitutionally vague and overbroad and violated his freedom of association.²²

The court began by noting that under a traditional First Amendment analysis, even if the government may constitutionally impose content-neutral prohibitions on a particular manner of speech, it may not condition that speech on obtaining a license or permit from a government official who possesses boundless discretion.²³ Instead, the First Amendment is more tolerant of subsequent criminal punishment of speech than it is of prior restraint of that same speech. Therefore, a prior restraint

19. See *Bernstein v. State*, 974 F. Supp. 1288 (N.D. Cal. 1997) [hereinafter "Bernstein III"].

20. The *Berstein* case was originally filed prior to the transfer of non-military encryption products to the jurisdiction of the Commerce Department.

21. *Bernstein III*, 974 F. Supp. at 1293.

22. *Id.* In the first *Bernstein* opinion (*Bernstein I*), the court held that source code constituted speech for purposes of the First Amendment and concluded that Bernstein's claims presented a colorable constitutional challenge. *Bernstein v. United States Department of State*, 922 F. Supp. 1426 (N.D. Cal. 1996). On appeal (*Bernstein II*), the court held that the licensing requirements under the ITAR constituted an unlawful prior restraint and invalidated parts of the regulations. *Bernstein v. United States Department of State*, 945 F. Supp. 1279 (N.D. Cal. 1996). After *Bernstein II*, the jurisdiction over export controls was transferred to the BXA. Bernstein then filed an amended complaint arguing that the new regulations (EAR) also constituted an unconstitutional prior restraint.

23. *Bernstein III*, 974 F. Supp. at 1304.

comes with a heavy presumption against constitutional validity.²⁴ In this Bernstein appeal, the government contended that the encryption source code did not constitute speech at all because of its inherently functional nature. Thus, according to the government, encryption source code is not expressive and is not entitled to First Amendment protection. The court disagreed with this conclusion and observed that even though encryption source code is highly functional, it is nevertheless speech—functional speech. According to the court, computer programming is “not just a way of getting a computer to perform operations, but rather . . . is a novel formal medium for expressing ideas about methodology.”²⁵ The court reasoned that, by requiring prior governmental approval before engaging in these activities, the export restrictions clearly affected the common expressive activities of scholars (i.e., teaching, publishing, speaking and writing to colleagues concerning encryption technology). Further, these export restrictions created a high risk of self-censorship and/or censorship by the governmental decision-makers. The court did not rule out the possibility of regulating the technology for purposes of protecting national security, but added that if regulation is directed to expressive activity, then it must contain adequate safeguards in order to pass constitutional muster. What this means is that, at minimum, the licensing scheme must: 1) provide a decision within a specific and reasonable period of time; 2) provide for prompt judicial review; and 3) place the burden on the censor to justify the license denial.²⁶

Applying these minimum standards, the court concluded that the EAR did not provide adequate constitutional safeguards because the time limit for the internal appeals process was indefinite. There was no clear standard for reviewing license applications and the entire process was not subject to judicial review. Merely justifying the denial of a license application by stating that it is “contrary to national security and foreign policy interests” was, according to the court, an illusory and unconstitutional restraint.²⁷

Interestingly, in a factually similar case, a different court deter-

24. *Id.*

25. *Id.* at 1305 n20.

26. *Id.* at 1308.

27. *Id.* The court further stated that while

[i]t is mindful of the problems inherent in judicial review of licensing decisions regarding cryptographic software, both with respect to the sophistication of the technology and the potentially classified nature of the licensing considerations, there must still be some review available if the export controls on cryptographic software are to survive the presumption against prior restraints on speech.

Id.

mined that the EAR did not violate First Amendment rights.²⁸ Peter Junger, a law professor, sought to post various encryption programs on his academic web site. Under the export regulations, unless very complex precautions are taken, almost any posting of materials on an Internet Website is considered an "export" of the materials. Junger applied to the Commerce Department requesting a determination as to whether the items he sought to post were restricted by the export regulations. The Commerce Department determined that four of the five software items he submitted were subject to the export restrictions, but the first chapter of a textbook discussing encryption would not be so restricted. Junger then filed suit seeking an injunction and declaratory relief, arguing that the EAR violated rights protected by the First Amendment.

The court in *Junger* began by considering whether encryption code is expressive material. The court explained that certain software is inherently expressive as it contains an "exposition of ideas."²⁹ However, other software is inherently functional and users look to the performance of tasks by the software rather than the methods employed or software language used.³⁰ The court observed that computer software is especially functional if it is designed to enable a computer to do a designated task such as carrying out encryption, and is indistinguishable from dedicated computer hardware to carry out that same function. In short, "the value comes from the function the source code does."³¹ Although the court acknowledged that source code can occasionally have communicative elements, "merely because conduct is occasionally expressive does not necessarily extend First Amendment protection to it."³² Encryption code is not overwhelmingly and unmistakably expressive and is not designed to communicate ideas, so the court concluded that the export regulations did not constitute an unconstitutional prior restraint on expressive conduct.

Alternatively, Junger argued that the EAR discriminated against encryption software by imposing export regulations on the software which suppressed, disadvantaged or imposed differential burdens on speech based upon its content. Junger further contended that this content-based regulation required a strict scrutiny standard of review by the court. In response, the court determined that the export regulations are not content based because the regulations impose burdens on encryption software without reference to any views it may express. Instead, encryp-

28. *Junger v. Daley*, 8 F. Supp. 2d 708 (N.D. Ohio 1998). The *Junger* case was filed after the transfer of jurisdiction for nonmilitary encryption products to the Commerce Department.

29. *Junger*, 8 F. Supp. 2d at 716.

30. *Id.*

31. *Id.*

32. *Id.* at 717.

tion software is regulated "because it has the technical capacity to encrypt data and . . . jeopardize American security interests," not because of its expressive content.³³

After finding that the export regulations were content neutral, the court evaluated the EAR using an intermediate level of scrutiny. Under this analysis, the export regulations could pass constitutional muster if they furthered a substantial governmental interest, were unrelated to suppression of free expression, and if the incidental restriction of First Amendment rights was no greater than essential to the furtherance of that interest. The court determined that, in the area of export controls, the government's substantial interest was evidenced by the need to control the export of encryption software to potentially hostile countries or individuals in order to protect vital national security interests. The court added that, "The use of encryption products by intelligence targets can have a 'debilitating' effect on the National Security Agency's 'ability to collect and report' . . . critical foreign intelligence."³⁴ Analyzing whether the regulations were unrelated to the suppression of free expression, the court held that the regulations were not designed to limit the free exchange of *ideas* about cryptography, but only the software that does the actual function of encrypting data. Lastly, the court found that the licensing requirements were tailored to address the risks posed by allowing unrestricted export of the technology and left open ample alternatives for communication of cryptography ideas, e.g., written communication.

These cases are examples of the courts' most recent attempts to interpret federal regulations restricting the export of encryption software. Although the courts in these examples reached different conclusions as to whether the restrictions violate first amendment standards, both courts acknowledged the vital national security interests that might be jeopardized by the unrestricted export of encryption technology. The courts further recognized that, under certain circumstances, the government may burden expressive activity to protect legitimate governmental interests. In addition to challenging the validity of the export regulations in the courts, various business and citizen groups have consistently pressured the Clinton administration to relax the export controls in order to allow the U.S. to remain competitive in the e-commerce arena.³⁵

33. *Id.* at 720. The court concluded that because publicly available information used to design or operate encryption products could still be freely exported, the export regulations are not directed at the content of ideas. *Id.*

34. *Id.* at 722. The court reasoned that even though encryption products are already available in some foreign jurisdictions, the U.S. government nevertheless has an interest in limiting further distribution. *Id.*

35. In early 1998, Commerce Secretary William M. Daley announced that the Clinton Administration encryption policy had been a failure and had resulted in a stalemate be-

In response to this pressure, the Administration has essentially adopted a piecemeal approach to relaxing the encryption export standards. The most recent encryption policy pronouncement from the Clinton administration has further relaxed the export standards as they relate to certain industries. According to Vice-President Al Gore, the updated policy reflects the "difficult task of balancing commerce and privacy interests against the needs of law enforcers who fear that unfettered export of encryption will aid criminals and terrorists."³⁶ Hailed as a "balanced approach" to one of the most important and challenging issues of our time, the new federal policy places more institutions under the umbrella of the expanded export treatment already in place for banks and financial institutions.³⁷

For example, the new policy adds insurance companies to the definition of financial institutions entitled to receive expanded treatment under the export regulations. The policy also provides that encryption products of any key-bit length can be exported to health and medical organizations (excluding biochemical/pharmaceutical manufacturers) in a list of 45 enumerated countries. Online merchants in the 45 listed countries are also included in the relaxed treatment standards in order to ensure more secure e-commerce transactions between those merchants and their customers. Finally, the new policy provides for the export of strong encryption of any key-bit length to the subsidiaries of U.S. companies in the 45 select countries. The policy left intact the ability to freely use any strength encryption products within the United States.

In the press conference announcing the expanded encryption export standards, representatives of the U.S. government emphasized that progress on these issues was made possible because "industries, agencies and Congress sat down together, pulled the problem apart, began to look at its different components and began to fashion very pragmatic solutions." Indeed, the expanded encryption policy reflects a compromise resulting from lengthy and often contentious debates concerning the competing interests of national security and the need for a secure environment to promote the rapidly growing Internet economy. In the words of Vice-President Gore, the new policy would "dramatically [increase]

tween the competing interests of law enforcement and the information technology industry. Daley further observed that the United States' restrictive policy had encouraged the growth of foreign producers of encryption products while retarding such growth in the U.S. See, *Administration's Encryption Policy is Failure, Daley Admits in Releasing E-Commerce Report*, 64 Telecommunications Rep. 16 (April 20, 1998).

36. Vice President Gore made these remarks at a White House press briefing on September 16, 1998.

37. Banks and financial institutions had already been allowed to export strong encryption products provided their use was limited to protecting the security of financial transactions.

privacy and security for families and businesses without endangering our national security.”

Despite these expanded standards, however, there are many who argue that the Administration’s encryption policy is still too restrictive and should be relaxed even more in order to allow for secure global communications and further encourage e-commerce over the Internet. In fact, on the legislative front, several bills have been introduced in Congress to further ease encryption export restrictions. Proponents of the legislation, including several high-tech companies, Internet users and civil liberties organizations argue that the current export controls unfairly favor software companies outside the U.S. and simultaneously result in inadequate protection for the privacy interests of U.S. citizens desiring an active role in the e-commerce revolution. These same groups are equally critical of the administration’s piecemeal approach to relaxing export controls, contending that the administration is pursuing a divide and conquer strategy that will eventually leave only average and non-corporate users without the benefit of strong encryption.

One of the primary areas of controversy surrounding the proposed legislation involves the government’s persistent requirement that any expansion of encryption controls be accompanied by “back door” access, which would allow the government to “crack the code” of any encrypted message.³⁸ Opponents argue that back door access will be a strong disincentive for non-U.S. companies to purchase the software and will only increase the foreign competitive advantage by providing more business for software companies outside the U.S. that do not impose such a requirement. In response to this argument, the government again relies upon the significant criminal and/or terrorist threat to national security to support its contention that any expansion of encryption controls should also include a “back door” or key escrow/key recovery system. Not surprisingly, the idea of key escrow or key recovery is exceptionally controversial because it would provide the government with the ability to decrypt confidential communications if it believed these communications were used for criminal or terrorist purposes. In addition to the privacy concerns raised by potential governmental access to private communications, there are several practical difficulties associated with establishing such a key escrow/recovery system on a widespread basis. For example, who will maintain the keys? Public or private entities? What standard, if any, will be required before the government will be allowed access to the private keys? Who will certify/police the keepers of the keys? These implementation concerns have led some to conclude that a key escrow/

38. It is however noteworthy that the Administration’s most recent updated encryption policy eliminates the requirement for key recovery plans or key recovery commitments for export of 56-bit encryption products.

recovery system would itself be vulnerable to attack and infiltration and would therefore exacerbate rather than alleviate the potential for criminal activity. More specifically, critics contend that the collection and storage of private keys in the hands of government or private entities would be susceptible to technical attack as well as abuse through mistake or corruption. Given the controversy and unanswered questions, the issue of back door access through a key escrow/recovery system is typically a pivotal and hotly contested issue in any discussion involving the expansion of encryption controls. Additionally, because encryption is part of the digital signature process, the issue also arises in discussions concerning the need to develop universal digital signature technology standards.

IV. DIGITAL SIGNATURES LEGISLATION

Recognizing the need to promote secure electronic communication, many states have adopted laws regulating digital signature technology and certification authorities.³⁹ Unfortunately, but perhaps predictably, these laws take vastly different approaches to critical issues surrounding the evolving technology.⁴⁰ In fact, the various state laws run the gamut from minimalist enabling legislation to far reaching regulatory schemes which restrict technology to digital signatures using public key cryptography and licensed certification authorities. The multitude of state statutes regulating digital signature technology creates numerous difficulties. First, because states have varying standards for authentication and certification authorities, individuals participating in interstate e-commerce transactions cannot be certain that an electronically signed document will be given the same recognition in every jurisdiction. Second, foreign jurisdictions conducting business with individuals in the United States would necessarily have to acquaint themselves with the variety of state standards and procedures governing the authenticity and validity of digital signatures. Finally, and perhaps most importantly, the variety of state laws and the inconsistency in their provisions create an atmosphere of confusion and untrustworthiness that may ultimately impede the overall expansion of e-commerce.

39. Utah was the first state to legally recognize the validity of digital signatures as an acceptable substitute for written signatures. Since that time, more than 30 states have either enacted or begun developing digital signature laws.

40. For example, the Utah statute is technology specific and recognizes only public key based digital signatures. In contrast, California's law recognizes both public key cryptography and signature dynamic technology. State statutes also differ in the scope of recognition for digital signatures. For instance, many state digital signature statutes provide that digital signatures will only be recognized in connection with or between governmental agencies.

To overcome these difficulties, many have called for federal statutory intervention to establish a digital signature standard for e-commerce transactions within the United States. Such legislation would establish uniform standards for digital signature technology in order to ensure that digital signatures are universally accepted and have the same legal standing as written signatures in every jurisdiction in the United States. One of the first steps toward uniformity in the area of digital signatures occurred when the Electronic Financial Services Efficiency Act of 1997 was introduced into the House of Representatives in late 1997.⁴¹ According to one of the sponsors of the bill, its purpose was to provide for the recognition of digital and other forms of authentication, improve efficiency and soundness of capital markets and payment systems, and harmonize the practices, customs and uses applicable to electronic authentication on a uniform national basis. Under the provisions of the bill, digital signatures would be considered valid for electronic communications with federal agencies, United States courts and other agencies of the United States government. Additionally, unless prohibited by state law, digital signatures for all other types of electronic communication would be valid as well. The legislation also sought to establish the National Association of Certification Authorities, which would serve as a national registration agency for anyone seeking to provide electronic authentication services in the United States.

Another bill, the Digital Signature and Electronic Authentication Law ("SEAL") of 1998, was introduced into both houses of Congress in early 1998.⁴² SEAL was described as a minimalist approach to federal action in the area of digital signatures as compared to other pending federal legislation. The purpose of SEAL was to authorize financial institutions to use electronic authentication in business transactions unless such use was inconsistent with or threatened the safety and soundness of the institution. The legislation also prohibited state government entities from acting as digital certification authorities or imposing fees with respect to electronic authentication services for financial institutions. The limitation on state government entities was intended to avoid uneven and conflicting state laws that might hinder the financial institutions' ability to provide customer security and system integrity.

Despite these legislative attempts, some argue that even the minimalist legislation goes too far and that the federal government should adopt a "bare bones" approach that simply creates a climate to encourage the use of digital signatures and ensure that digital signatures are granted the same legal standing as written signatures. Such an approach would enhance consumer confidence in digital signature technol-

41. H.R. 2937, 105th Cong., 1st Sess. (1997).

42. H.R. 3472, 105th Cong., 2d Sess. (1998); S. 1594, 105th Cong., 2d Sess. (1998).

ogy while clearly not preempting the numerous state legislative efforts that are already in place. At present, neither the expansive nor minimalist approach to federal legislation is prevailing since much of the legislation in this area is apparently stalled in the congressional committee process. Although there are perhaps myriad reasons why the federal government has not adopted a national uniform digital signature statute, given the complex intermingling of digital signatures, encryption, Internet commerce and national security issues, it does not require a great leap of imagination to conclude that the failure to untangle these distinct issues may be part of the problem.

V. THE ROAD TO A NATIONAL DIGITAL SIGNATURE POLICY

Given the rapidly expanding global Internet economy and the increasing demand for a secure method to conduct e-commerce transactions across the Internet, it is imperative that the United States adopt a national uniform digital signature law. Although states have led the way in adopting digital signature statutes, a national policy would encourage growth of the Internet economy while providing uniform standards for interstate and international e-commerce transactions. There are several key issues that must be clarified and resolved before such a national policy becomes a realistic alternative.

First, there must be a recognition and understanding that digital signature technology is *not* synonymous with encryption technology. As explained above, digital signatures utilize public key encryption technology as part of the process of transmitting secure and authentic communications across networks. Thus, while encryption and security are important aspects of the digital signature process, the primary purpose of a digital signature is to ensure that a particular transaction originated from a specific person or entity and has not been altered during its transmission. In short, digital signatures ensure authentication and integrity of communications in online transactions and thereby significantly reduce the potential for fraud and/or later repudiation. Thus, although the digital signature process uses encryption technology, this particular use of encryption does not pose a significant threat to national security or law enforcement objectives because encryption technology is not used as a means to secure confidentiality, but as part of the digital signature verification process. With digitally signed documents, questionable Internet communications are easily traceable to their origin where there would presumably be unencrypted or plain text copies of the transmission. Because of the extremely limited and inherently traceable uses of encryption technology in digital signature applications, concerns about criminal or terrorist uses of encryption in this process are largely misplaced. Thus, an essential prerequisite to establishing a national digital

signature policy is to clarify, understand and differentiate the entirely benign use of encryption technology in the digital signature process.

Nevertheless, because encryption is still a part of the digital signature process, any proposal for a national standard will inevitably have to confront the issue of key access or key recovery systems. If the purpose of key access/recovery is to enable decryption of suspected criminal transmissions, then that concern should be minimal in the digital signature context because, in most instances, a digitally signed message will have certain identifiable characteristics and be traceable to a specific individual or entity in much the same way that a traditionally signed document can be traced to the parties entering into an agreement. Moreover, the inherent ability to trace a digitally signed message is likely to act as a strong deterrent to using encryption in this manner for criminal or terrorist purposes. Although making strong encryption available for use in the digital signature process may result in a greater potential for criminals to access strong encryption products, as a practical matter, criminals already have access to strong encryption products sold *outside* the United States and there is no way to completely prevent those with criminal designs from ever gaining access to such strong encryption products. Restricting the export of strong encryption technology used in the digital signature process or conditioning its export on establishing widespread key recovery systems will foster public apprehension about the process and impede entry into the realm of e-commerce, while providing little corresponding benefit in terms of protecting national security. Considering the fact that most digitally signed documents are likely to be part of legitimate business transactions, a less costly and less restrictive alternative to a key recovery system would favor reliance on the unencrypted original documents which are likely to remain in the possession of the parties to the transaction.⁴³ Another alternative might be technologically limiting the functionality of encryption within the digital signature process. To the extent that the encryption software can only be used for purposes of authenticating and verifying the user of a digital signature, there will be a strong disincentive for criminals to use the technology because there would be no guarantee of absolute confidentiality in the communication.

Since digital signatures are used primarily to authenticate and verify the identities of parties to transactions, the expansion and widespread acceptance of digital signature technology would also seem to require the establishment of independent entities to guarantee or certify the identity of the parties (key holders) and further enhance trust and confidence in the digital signature process. Simply put, in order to en-

43. A somewhat related alternative is user-controlled key recovery whereby users maintain a spare key for their own use or for the use of others should the need arise.

courage reliance upon digital signatures as a replacement for their written counterparts, parties must be able to trust that the digital signature is valid and owned by the party signing the document. Certification authorities ("CAs") are therefore a necessary component in the development and legal acceptability of digital signatures.⁴⁴ CAs would authenticate the ownership of a public key and issue a digital certificate that guarantees the identity of the signature holder as well as the validity of the signature.⁴⁵ An individual participating in a particular transaction could therefore rely upon the digital certificate as a means of insuring the identity of the parties to the transaction as well as the authenticity of their signatures. To ensure that digital certificates are indeed reliable, CAs must impose at least some minimal standards for verifying identities prior to issuing digital certificates and must have basic procedural safeguards to minimize the possibility of fraud and/or corruption. A uniform federal digital signature policy could create a standard licensing scheme for public and/or private entities seeking to become CAs and require that they carry out certain standard procedures for issuing certificates. While acknowledging that CAs are a critical component of the digital signature evolution, business groups and political entities currently cannot agree upon whether CAs should be private entities or regulated by the government.⁴⁶ Additionally, there is significant controversy on the issue of whether CAs would be required to maintain private keys (subject to surrender to government agencies upon lawful request) for any public key certified by the CA.

A national digital signature policy should also outline the precise legal effects of a digital signature. To fully encourage the use of the technology, digital signatures should be afforded the full effect and incur the same legal obligations as written signatures. So although a transaction may take place across miles of network cable, parties to a digital signature transaction should clearly understand that by transmitting a digital

44. Trusted third parties (TTPs) can also perform the role of authenticating and verifying the identity of keyholders. However, some classify TTPs as entities that would permit lawful access to encryption keys.

45. Such a guarantee would mean that CAs would have legal obligations to anyone who reasonable relies upon the digital certificate issued by the CA.

46. It is noteworthy that banks have recently taken the lead in beginning to establish themselves as digital certification authorities. For example, in 1998, Zions Bancorp of Salt Lake City, Utah became the first U.S. bank to offer CA services. Other financial institutions are also scrambling to establish themselves as CAs in an attempt to capture the enormous profits expected to flow from the growth of e-commerce. However, some fear that banks could gain a monopoly on CA services and argue that anyone who meets the capital and legal requirements for offering such services should be allowed to do so. This would include the possibility of self-certification, which means that a company could issue digital certificates and back them up with its own guarantee.

signature, they are bound just as if they had signed the document in person.

Finally, a uniform law should articulate when and under what circumstances the government would be able to gain access to public/private key or digital certificate information. The standards might also specify which entities (e.g., CAs) will be subject to government jurisdiction and what type of information they will be required to surrender to the government upon lawful request. Given the types of individuals and entities likely to use digital signature technology in online e-commerce transactions, it does not appear at this point that the established laws regarding search and seizure would need to be altered or reworked in order to address potential criminality in the online commerce setting. In fact, because digital signatures are used primarily for verification and authentication rather than criminal purposes, when there is a need for lawful governmental access to documents, there is perhaps a greater likelihood that those involved in the process will be predisposed to cooperate with lawful and necessary governmental objectives.

VI. CONCLUSION

Current federal government regulations and policies on strong encryption products are impeding the development and widespread use of related digital signature technologies that rely upon encryption for verification and authentication purposes. The expansion of e-commerce transactions and the tremendous opportunities and benefits available to merchants and consumers will not be realized unless there are mechanisms to ensure that online transactions are authentic and verifiable. Digital signatures clearly provide that mechanism. Thus, it is incumbent upon the federal government to take the lead in promoting entry into the global Internet economy by establishing minimal uniform standards that provide legal recognition for digital signatures. This task will first require an understanding that the limited use of encryption in the digital signature process is benign and non-threatening to law enforcement and national security interests. This understanding should enable digital signature technology to forge ahead unencumbered by the contentious debate that often surrounds encryption technology that is used solely for purposes of maintaining confidentiality. Next, in order to avoid confusion and inconsistent application and recognition of digital signatures, the federal government must enact a uniform federal statute that establishes basic guidelines to ensure universal and consistent recognition of digital signatures. Such a standard will encourage merchants and consumers both within and outside the United States to confidently participate in the Internet economy by providing a trustworthy environment in which to conduct online transactions.

