LEGAL ISSUES IN CRYPTOGRAPHY

by

Edward J. Radlo

Partner, Fenwick & West LLP

Palo Alto, California

March 1997

TABLE OF CONTENTS

INTRODUCTION

This article first sets forth a few technical concepts and definitions, then explores some of the more important legal and policy issues pertaining to cryptography. These issues include the allegation by the U.S. software industry that it is being harmed vis-à-vis its foreign competition due to the existence of overly harsh U.S. export control laws.

DEFINITIONS

As used in this article, "encryption" means a technique for converting a message into a secret form. The more general concept of "cryptography" includes not just encryption, but also authentication, which in turn comprises paternity, integrity, and non-repudiation. Related topics include key certification, key management (the generation, transmission, and storage of keys), key escrow, and public key infrastructure. "Plaintext" is a message before it is encrypted. "Cyphertext" is a message after it has been encrypted. "Cypher" is the method or device that performs the encryption; a cypher can be a mathematical algorithm. "Key" is analogous to a mechanical key that unlocks a mechanical door, i.e., it is the means to activate the cypher. In mathematical cryptography, a key is a word containing a certain number of bits. This number is called the "keylength" or "keyspace". A "digital signature" is the means by which public key cryptography accomplishes the task of authentication.

HISTORY OF CRYPTOGRAPHY

The first known uses of cryptography (by the Egyptians and Phoenicians) date back to about 2000 B.C. Cryptography historically had its biggest use in military applications. This was true up until the end of World War II. About the year 1900 A.D., mechanical cypher systems began to be invented. Starting around the year 1950, computerized cryptographic systems came into being. About that time, cryptography began to emerge as a branch of mathematics.

Cryptography was very important in World War II. For example, when the Allies broke the German ENIGMA cryptographic scheme, they obtained a major advantage that helped them win the war. An actual ENIGMA machine is on display at the National Museum of American History, part of the Smithsonian Institute, in Washington, D.C.

After World War II, cryptography was instrumental in the U.S. government's prosecution of Julius and Ethel Rosenberg for divulging the secret of the atomic bomb to the Soviet Union. Evidence that the Rosenbergs had spied on the U.S. atomic bomb program on behalf of the Soviet Union had been obtained from the U.S. government's VENONA program (1943-1948). The Rosenbergs were convicted in 1951. The role that cryptography played in this case was kept classified for 50 years as an official secret of the U.S. government. In 1995, it was finally divulged that the Rosenbergs, while attempting to use "one-time pad" encryption, *infra*, were careless in doing so, and didn't really use a one-time pad after all. This enabled the government to develop evidence that assisted in their conviction.

CURRENT USES OF CRYPTOGRAPHY

Cryptography is currently receiving increasing attention as we transition into a world of widespread digital communications. Cryptography is widely seen as the essential means for securing the *privacy* of communications over digital media. Thus, cryptography can provide the basis for secure electronic commerce, including secure telephone conversations, scrambled television broadcasting, private e-mail, and sending one's credit card number over the Internet in a confidential manner. Cryptography can also provide the means for establishing the *authenticity* of a document. This authentication feature has three major aspects: 1) proving that the person who claims to have signed the document actually did so ("paternity"); 2) proving that the document was not altered since signature ("integrity"); and 3) preventing a digital signer from later asserting that he or she didn't sign ("non-repudiation"). The authentication feature is used to verify electronic (digital) cash. In public key cryptography, authentication is accomplished by a technique known as "digital signatures".

DIGITAL SIGNATURE LEGISLATION

In May 1995, Utah became the first political entity in the world to adopt a digital signature statute.[1] The State of Washington, the County of Los Angeles, and some foreign jurisdictions have followed suit. For example, Germany recently enacted digital signature legislation. Chile has a proposal for the same. Japan, China, and France do not have digital signature laws as of yet. However, in France, judges can authenticate digital signatures on a case-by-case basis.

In the Utah legislation, the private key is extremely strong. This provides great risks, should the private key be lost, stolen, or compromised. As to the question of liability of certificate authorities (CA's), e.g., for erroneously binding someone to a public key, the Utah legislation provides a safe harbor of reduced liability for qualifying CA's. However, as of this writing, no CA's have so qualified. Generally speaking, the question of liability for CA's is important, controversial, and unsettled. Principles of contract law and tort law have to be examined in determining the liability of a CA in a particular case.[2]

The American Bar Association's Science and Technology Section published a comprehensive Digital Signature Guidelines in August 1996. The United Nations has established a study group on digital signatures.

California's digital signature law was enacted in October 1995.[3] It covers the use of digital signatures in non-mandatory filings with government agencies. Liability for fraud is typically placed on the party that holds the private key, because it is deemed that that party is in the best position to prevent the fraud. The California Secretary of State was supposed to have promulgated regulations implementing the statute by January 1, 1997, but by March 1997 had not done so.

PRIVATE KEY (SECRET KEY) CRYPTOGRAPHY

Up until the mid-1970's, the only type of cryptography that was available was one using private keys (secret keys). In private key cryptography, the key for encryption is the same as the key for decryption. Thus, a private key cypher is sometimes

referred to as a "symmetric" cypher. Because of this symmetry, the sender and the receiver must both know the key. If the key must be transported from the sender to the receiver, then secure means, e.g., a trusted courier, must be employed.

In 1949, the famous mathematician Claude Shannon proved that one and only one cypher (the one-time pad) is absolutely unbreakable. In the one-time pad, the key is used one time only, and then it must be discarded. Modern cryptographic techniques, whether private key or public key, are theoretically breakable; but work on the basis that if the key is sufficiently large (i.e., the key has a large number of bits), it would take even the fastest supercomputer so many years to break the system that it is virtually unbreakable. A cryptosystem having this characteristic is known as "strong".

Other than the one-time pad, examples of private key cryptosystems include the U.S. Data Encryption Standard (DES), Skipjack, RC2, RC4, and IDEA.

DES

The U.S. Data Encryption Standard (DES) is the world's most widely studied cryptographic system. It was jointly developed by IBM and the National Security Agency (NSA) in 1974, and adopted as a Federal Information Processing Standard (FIPS) in 1977. It was patented in the U.S. DES works on the basis of 64-bit blocks of data, and uses a 56-bit randomly generated key. There are 2^{56} keys to choose from. The use of triple-DES (DES used three times on the plaintext) gives an effective 112-bit keyspace. In general, for any cryptosystem, the longer the keyspace, the stronger the cypher.

SKIPJACK

The Skipjack algorithm also operates on 64 bits of blocked data, and uses an 80-bit keyspace. The Skipjack algorithm is the heart of the Clipper Chip, the U.S. government's controversial means for providing a "back door" that enables the government to eavesdrop on otherwise confidential communications under certain circumstances. Skipjack is a secret, classified algorithm (unlike the algorithm in DES and unlike the RSA public key algorithm, *infra*); it was written by the National Security Agency.

OTHER PRIVATE KEY ALGORITHMS

RC2 stands for Ron's Cypher 2, and RC4 stands for Ron's Cypher 4. Ron is Dr. Ronald Rivest, one of the inventors of the RSA public key algorithm (see *infra*). RC2 and RC4 are trade secrets, but the secrecy on RC4 has been compromised due to its having been disseminated on an Internet Usenet newsgroup.

IDEA (International Data Encryption Algorithm) was invented by James Massey and Xuijia Lai of Zurich, Switzerland. It uses a 128-bit key, and is a building block of PGP, *infra*.

PROBLEMS WITH PRIVATE KEY CRYPTOSYSTEMS

There are three major drawbacks to private key cryptography. The first major drawback is that a secure channel is needed for the parties to agree on the key and to

transport the key. The second major drawback is that each two people communicating using private key cryptography need their own unique key. This can quickly add up to an unwieldy number of keys if many people are using the cryptographic scheme. The third major drawback of private key cryptography is that it cannot perform authentication on an open network.

On the other hand, private key cryptography is relatively faster than public key cryptography.

PUBLIC KEY CRYPTOGRAPHY

Public key cryptography was invented in 1976 and overcomes the above three major problems inherent in private key cryptography. In public key cryptography, there are two keys: a public key that is publicly disseminated, and a related private key that remains known to just the user. It is not intentionally shared with anyone, although a third party, such as the user's employer, may have the right to access it under certain circumstances. Those wishing to be the recipients of encrypted messages post their public keys in a public place, like the Internet, and senders use the recipients' public keys to encrypt the plaintext messages.

The major drawback of public key cryptography is that it is relatively slow compared with private key cryptography. This problem can be overcome in part by combining public key cryptography with private key cryptography. For example, public key cryptography can be used to exchange a "session key" for a particular communications session; then most of the communications are subsequently conducted using the faster private key cryptography, with the session key as the single key.

The field of public key cryptography was launched by a paper published by Whitfield Diffie and Martin Hellman in 1976.[4] The Diffie-Hellman concept, important as it was, did not go so far as to invent a practical means of achieving public key cryptography. That seminal event happened in 1977 when three professors from the Massachusetts Institute of Technology (MIT) æ Ron Rivest, Adi Shamir, and Len Adelman æ invented what is called the RSA algorithm after their initials. This invention is protected by a patent owned by MIT.[5] This patent is exclusively licensed to a company called RSA Data Security, Inc. (RSA).[6] The MIT patent was the subject of litigation, *infra*. The RSA algorithm works on the basis that, whereas it is a trivial matter to multiply two large numbers together, whether or not they are prime numbers, it is an exceedingly difficult operation mathematically ("computationally infeasible") to factor a large number into two or more prime numbers.

PGP

Other well known public key cryptosystems include PGP, which is the most widely used non-commercial cryptosystem, and ViaCrypt, a commercial version of PGP. PGP stands for "Pretty Good Privacy". It was invented in 1991 by Phil Zimmermann. PGP is a combination of the RSA public key algorithm and IDEA. In May 1996, ViaCrypt sold the commercial rights of PGP back to Mr. Zimmermann, who started his own company, Pretty Good Privacy Inc.

USING PUBLIC KEY CRYPTOGRAPHY

Running a public key crypto-engine in forward results in encrypting a message, thereby achieving the first goal of cryptography, i.e., privacy. Running a public key crypto-engine in reverse achieves the second goal, namely authentication. "Running in forward" means encrypting the plaintext using the recipient's public key. The recipient then decrypts the cyphertext by using his or her own private key. "Running in reverse" means encrypting the plaintext using the sender's private key (rather than the recipient's public key), or, preferably, encrypting an abbreviated version of the plaintext called a "message digest"[7], which is made by applying a "hash function" to the plaintext. Examples of well-known hash functions are MD4, MD5, and SHA. The recipient then decrypts the message digest using the sender's public key.

Various schemes have been proposed to certify the authority of public keys, to guard against forgery of the public keys ("spoofing"). These schemes are part of the general subjects known as "key management", "key certification", and "public key infrastructure" (PKI). Examples of certification authorities operating nationally are Verisign and the U.S. Postal Service. There are currently 45 pilot PKI projects being conducted within the U.S. government, as well as a federal public key infrastructure Steering Committee. The U.S. government envisions an international public key infrastructure comprising an interlinked network of hierarchical legalized certification authorities. This has been criticized by many commentators as being unnecessary. Alternatives include the "web of trust" used by PGP aficionados to exchange encrypted e-mail over the Internet.

Because public key cryptography entails the wide dissemination of public keys, it is ideally suited for a communications medium that is public, e.g., the Internet. Many of the companies that are trying to exploit the Internet economically thus use public key cryptography. For example, Terisa, a joint venture of RSA and Enterprise Integration Technologies (since acquired by Verifone), uses the RSA public key algorithm, as does Netscape Communications, CommerceNet, and scores of others.

MAJOR LEGAL ISSUES

A company interested in manufacturing or marketing a product that implements a cryptographic function must be aware of several important legal and policy issues. Some of these issues are highly controversial and continue to generate a lot of public attention, particularly the existence and construal of the export control laws of the United States, and the promulgation of Federal Information Processing Standards (FIPS). International laws, regulations, and customs must be considered. Another issue that will be touched on briefly in this paper is that of standards set by industry and non-U.S. groups. A fifth issue, patents, has also engendered controversy, but has not attracted the same degree of press coverage as export control laws and Federal Information Processing Standards.

THE POLICY DEBATE

The last few years have witnessed a vigorous, sometimes acrimonious, debate within the United States on cryptography policy. Generally, government positions

have been opposed by most of industry and by civil liberties groups.

The U.S. government insists that it needs to maintain controls on cryptography, particularly encryption, for reasons of national security and law enforcement. It cites its continuing struggle against the "Four Horsemen of the Apocalypse" of the 1990's: terrorists, child pornographers, drug dealers, and spies, all of whom have used strong encryption to advance their criminal activities.

On the other hand, the vast majority of those wishing to use encryption do not fit into any of these categories. They argue that it is not necessary or fair for the government to severely restrict the vast, legitimate uses of cryptography in order to attack admitted societal menaces; and that more problem-specific laws could be formulated, such as increasing the penalty for those using cryptography in perpetration of terrorism, child pornography, drug dealing, or spying, while relaxing the general restrictions on cryptographic export. They argue that there is no recorded instance of where a U.S. law enforcement agency would have stopped a crime if the agency had decrypted something.

The point is repeatedly made that strong cryptographic "toothpaste is out of the tube" and widely known throughout the world. Thus, knowledgable criminals can rather easily circumvent existing and proposed regulations, meaning that only the innocent are thwarted by the government's policies. For example, hundreds of strong cryptographic products are marketed in Europe and Japan, some of which were illegally exported out of the United States and some of which were developed abroad.

It is also pointed out that strong encryption *protects* legitimate business and private communications *against* the attacks of criminals, thus creating jobs and strengthening the economy.

EXPORT CONTROL LAWS

The most significant way in which the United States government controls the use of cryptography by business and individuals is via the export control laws.

HISTORICAL ORIGINS

Until 1992, the export of virtually all cryptography was regulated by the U.S. State Department by the ITAR (International Traffic In Arms Regulations).[8] These Regulations were developed during the Cold War between the United States and the Soviet Union. Between 1992 and December 1996, the jurisdiction over cryptography exports was shared by the State Department and the Commerce Department. Since December 1996, most crypto exports have been regulated by the Commerce Department.

The statutory authority for the ITAR is the AECA (Arms Export Control Act).[9] The ITAR places controls on exports (to anyplace other than the United States or Canada) of "defense articles" and "munitions". In other words, up until December 1996, the U.S. government considered all cryptography, even cryptography used solely for commercial applications, and cryptography that was not classified, to be a defense article or munition. There were some exceptions, in which the State Department relinquished jurisdiction in favor of the Bureau of Export Administration (BXA) within the Commerce Department, for certain types of cryptographic products, typically those em-

ploying no or weak encryption, as will be discussed below. But, generally speaking, the State Department, both on its own volition and as advised by the the National Security Agency (NSA)[10], directly regulated the export of cryptography for reasons of national security. Generally, a cryptographic product under State Department jurisdiction was difficult or impossible to export, whereas a product under Commerce Department jurisdiction was possible to export, albeit with some restrictions.

NO PUBLIC DOMAIN EXEMPTION FOR SOFTWARE

Software in general is not exempt from the controls of the ITAR just because it is in the public domain (e.g., firmware or shareware).

The ITAR provides a public domain exemption for *information* that is published and that is generally accessible or available to the public, e.g., through sales at newsstands and bookstores, or through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information.[11] Also, the ITAR exempts from the definition of *technical data* that information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges, and universities; basic marketing information on function or purpose; and general system descriptions of defense articles.[12]

However, the ITAR makes a distinction between "technical data" and "information" on the one hand, and "software" on the other hand.[13] The State Department has construed the regulations in such a way as to effectively eliminate the public domain exemption for software *per se*. This was most poignantly done in the *Karn* case, *infra*.

Some exporters have relied on what they thought was a public domain exemption only to receive serious punishment after they exported their software. The case of *United States v. Hoffman*[14] upheld the conviction of Ronald J. Hoffman, a rocket scientist with expertise in rocket plume technology, who was found to have illegally exported a set of software programs called CONTAM. Hoffman unsuccessfully argued that "generally accessible" was broader than "available to the public" (see above definition).

The case of *United States v. Martinez*[15] upheld the conviction of two exporters for violating the Arms Export Control Act by non-licensed exports of video signal descramblers. The defendants unsuccessfully argued that placing all "cryptographic devices and software (encoding and decoding)" on the Munitions List was overbroad. The court held that the political question doctrine renders the propriety of an item's placement on the Munitions List a non-justiciable issue in federal court.

The penalty for violating the Arms Export Control Act by improperly exporting an item on the ITAR is severe: fines of up to $1 million for each violation, or imprisonment of up to ten years, or both.[16] It is the fear of this punishment that has prevented many cryptographic products from being exported.

COMMERCE DEPARTMENT JURISDICTION

Prior to December 1996, there were three methods by which United States individuals and companies that wanted to export cryptographic products could attempt to transfer jurisdiction from the State Department to the more lenient jurisdiction of

the Commerce Department. The first method was to claim a "personal use exemption" for the product. The second method was to file a request for Commodity Jurisdiction (CJ) under the criteria in the ITAR governing automatic transfer to the Commerce Department. The third method was to apply under the regulations providing for case-by-case transfer to the Commerce Department.

PERSONAL USE EXEMPTION

In February 1996, after a lengthy two-and-a-half year study period, the State Department finally enacted, for the first time, regulations[17] to provide for the temporary export of cryptographic products, including encryption software, for personal use, e.g., while temporarily traveling abroad. This personal-use exemption, which was modified by the December 1996 Commerce Department Regulations, contained five limitations, as follows:

1. The software must be used only in conjunction with a simultaneously temporarily exported cryptographic hardware product or a simultaneously exported item on the Commerce Control List (CCL).

2. The product must not be taken to certain prohibited countries which have been determined to breed terrorism, currently Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria.

3. The encryption product must remain in the possession of the exporting person. It cannot be used for copying, demonstration[18], marketing, sale, re-export, or transfer of ownership or control. The exporter must take precautions to ensure the security of the product. While in transit, the exporter must keep the product in his or her carry-on luggage or locked in baggage accompanying the exporter, which baggage has been checked with the carrier.

4. At the time of export from the U.S. and import back into the U.S., the cryptographic product must be with the individual's accompanying baggage or effects.

5. The exporter must submit the product to inspection upon the request of a U.S. Customs Officer, and must maintain certain detailed records for a period of five years from the date of each temporary export.

CRITERIA FOR AUTOMATIC TRANSFER TO COMMERCE DEPARTMENT

In April 1992, in response to pressure from the Software Publishers Association (SPA) and other groups, the ITAR was relaxed somewhat to allow the automatic transfer of jurisdiction to the Commerce Department for certain types of cryptographic software. In order to qualify for this treatment, the software had to fall into at least one of the following categories listed in 22 CFR § 121.1:

1. Restricted to decryption functions specifically designed to allow the execution of copy protected software, provided the decryption functions were not user-accessible.

2. Specially designed, developed, or modified for use in machines for banking or money transactions, and restricted to use only in such transactions. Machines for banking or money transactions include automatic teller machines, self-service statement printers, point-of-sale terminals, and equipment for the encryption of interbank transactions.

3. Employing only analog techniques to provide the cryptographic processing to ensure information security for certain specific band scrambling, frequency inversion, facsimile, restricted audience broadcast, and civil television equipment.

4. Personalized smart cards, using cryptography restricted for use only in equipment or systems exempted from the controls of the United States Munitions List.

5. Limited to access control, such as automatic teller machines, self-service statement printers, or point-of-sale terminals, designed to protect password or personal identification numbers (PIN) or similar data to prevent unauthorized access to facilities, but not allowing for encryption of files or text, except as directly related to the password or PIN protection.

6. Limited to data authentication, i.e., calculating a message authentication code (MAC) or similar result to ensure no alteration of text has taken place, or to authenticate users, but not allowing for encryption of data, text, or other media other than that needed for the authentication.

7. Restricted to fixed data compression or coding techniques.

8. Limited to receiving for radio broadcast, pay television, or similar restricted audience television of the consumer type, without digital encryption and where digital decryption was limited to the video, audio, or management functions. This criterion appeared to be a response to the *Martinez* case, *supra*.

9. Software designed or modified to protect against malicious computer damage (e.g., viruses).

The above categories have been essentially carried over to the December 1996 Commerce Department Regulations, meaning that it is currently relatively easy to obtain permission to legally export items that fit into one of these categories.

It should be noted that the Commerce Department has the authority to restrict or prohibit exports of all categories of goods to certain country groups, e.g., countries where there has been recent terrorist activity. Also, the Commerce Department places a record-keeping burden on all exporters, and sometimes requires written assurance from the importer that the product will be put to a legitimate use.

In July 1992, the State Department approved a new procedure to expedite Commodity Jurisdiction determinations for mass market software that had limited encryption capabilities (keyspace of 40 bits or less in the case of private key encryption).[19] "Mass market" software was defined as computer software that was available to the public at retail locations, through mail order transactions, or through telephone transactions. In addition, the software had to be designed so that the user could install it without substantial support from the supplier. Software products that did not meet the definition of "mass market", and did not meet the specified technical restrictions on their encryption capabilities, had to be reviewed using the case-by-case CJ procedure. It should be noted that by 1996, private key encryption with a 40-bit keyspace was considered weak, and had been broken with relatively modest computational power.

In May of 1995, the Commerce Department simplified procedures for export of mass market software with encryption features intended for testing purposes, by announcing a new general license, G-BETA. This relaxation in the regulations was due to lobbying by the American Electronics Association (AEA).

CASE-BY-CASE TRANSFER TO COMMERCE DEPARTMENT

In addition to the above, there was, prior to December 1996, a procedure for transfer to the Commerce Department for certain mass-market software products with data encryption capabilities. Such mass-market software had to satisfy all three of the following criteria:

1. The software had to be designed to run on microcomputers.

2. The software had to employ a non-standard cryptographic algorithm not of strategic value.

3. Encryption could not be the primary function of the software.

Definitions of "non-standard" and "not of strategic value" never appeared in the ITAR or in any regulations of the Commerce Department.[20] Furthermore, neither the State Department nor the Commerce Department has ever published any of its decisions permitting or denying the export of particular items of cryptography.

ADMINISTRATIVE AND JUDICIAL APPEALS

One who is denied a CJ from the State Department can apply for reconsideration, and, failing that, appeal first internally to the Director of the Office of Defense Trade Controls within the State Department, and, thereafter, to the Assistant Secretary of the Bureau of Politico Military Affairs of the State Department.[21] The Arms Export Control Act was amended in 1990 to state that there could be no judicial review of

whether or not an item was properly designated as a defense article or service,[22] thus making appeals much more difficult. A previous case, *United States v. Edler Industries*[23], had reversed the criminal conviction of an exporter who had not been allowed to produce evidence of non-military use of technical data, which evidence would have been relevant to the CJ determination.

DECEMBER 1996 COMMERCE DEPARTMENT REGULATIONS

In November 1996, President Clinton issued an Executive Order stating that "henceforth all encryption items currently on the U.S. Munitions List except those specifically designed, developed, configured, adapted or modified for military applications be transferred from the jurisdiction of the State Department to the jurisdiction of the Commerce Department".[24] The Executive Order was issued pursuant to the International Emergency Economic Powers Act, the Export Administration Act having expired in August 1994. This was controversial, there being no apparent international economic emergency in November 1996.

In December 1996, the Commerce Department promulgated two sets of regulations embodying this Executive Order: an Interim Final Rule giving guidelines for implementing key escrow[25] and an Interim Rule covering broader matters.[26] These regulations were issued without a notice of proposed rulemaking, the opportunity for public participation, and a delay in the effective date, all as required by the Administrative Procedure Act.[27] Again, this was highly controversial.

The Interim Rule made a few changes to the U.S. government's scheme of regulating crypto exports, while keeping much of the scheme intact.

The major change in the Interim Rule was to legalize the export of encryption software having a keyspace of up to 56 bits (i.e., the strength of DES) provided that the exporter files with the Commerce Department an approved plan for designing and implementing within two years a hardware and/or software system that will enable the government to recover the keys, and therefore obtain the plaintext of the encrypted message upon the showing of sufficient cause, presumably including the presentation of a search warrant. Previously, 56 bits had been permitted for export only to financial institutions and to foreign subsidiaries of U.S. companies. "Government key recovery" is similar to and slightly broader than the controversial concept of "government key escrow", described below.

Another change made in the new regulations is a broader and more express definition of "export". The definition now covers posting software on the Internet. Accompanying the definition is a new set of rules governing how the posting entity can protect itself from unwanted exports when posting on the Internet.[28]

The new regulations specifically allow the export of public key cryptography of up to 512 bit keyspace for exchange of a session key only, and then only if the underlying session key is 40 bits or less. This is the only mention of public key cryptography in the new regulations. Said regulations also permit the export of 64-bit symmetric encryption for exchanging session keys. This is the only point at which the regulations mention 64 bits.

The new regulations codify the CJ's that were issued by the State Department in the *Karn* case, *infra*, thus codifying the controversial ruling that it is permissible to

export books but not floppy disks containing source code listed in the books. Furthermore, accompanying the Regulations in a section entitled "Supplementary Information" is an ominous statement that "The administration continues to review whether and to what extent scannable encryption source or object code in printed form should be subject to the EAR and reserves the option to impose export controls on such software for national security and foreign policy reasons."

In other words, the government may in the future try to restrict the export of books that list computer source code. There are two possible scenarios here. The first scenario is that the book has already been published in the United States. In this scenario, the ITAR currently provides, as discussed above, for a public use exemption for such information. Thus, if the government attempted to so regulate in this scenario, it would be backtracking even from ITAR. Also, the government would have an extremely difficult time attempting to prohibit the subsequent export, given the First Amendment to the United States Constitution, which protects freedom of speech.[29] The second scenario is that the book has not been previously published in the United States. In this scenario, the entity desiring to export the book could simply first publish the book in the United States, converting the second scenario into the first scenario. The government would have great difficulties with attempting to restrain the publication in the U.S., since the First Amendment has routinely been applied to prohibit such prior restraints.

Another important distinction in the new regulations is that for the first time the Justice Department has an official role in determining whether cryptographic items can be exported. It is noted that the Director of the FBI, Louis Freeh, has publicly stated that the *use* of strong encryption *within* the United States should be restricted. The President and Vice President, however, have consistently stated that the Administration does not intend to do this, but rather will continue to control encryption via the export laws, as well as encourage use of government key escrow systems via Federal Information Processing Standards, export laws, and multinational agreements.

The government has treated "crypto with a hole" (hardware or software with no actual crypto but with the ready provision, in the form of a socket, hook, or application programming interface, for crypto to be plugged in) the same as if the crypto to be plugged in was actually present.[30] Another term for crypto with a hole is "crypto-ready" hardware or software, which can be analogized to a "cable-ready" television receiver.[31] The only support for the government's position in the ITAR was a vague statement that ITAR covers devices "modified" for military applications, as well as the enumerated military devices themselves. The new regulations somewhat clarify the situation regarding crypto with a hole, by providing that the export is not forbidden if 1) the encryption algorithm and associated key management routines are provided just in object code, not in source code; and 2) all calls to the algorithm are hidden.[32]

Finally, the new regulations replace the State Department regulations on the personal use exemption with a similar regulation providing for a general license BAG when the crypto stays with the baggage of the individual; and they add a general license TMP which allows for the temporary export of strong crypto for demonstration purposes. One wonders, however, how valuable it is to demonstrate a particular piece of crypto abroad if one is not allowed to sell it.

The recitation of penalties for violating Commerce Department export regulations is more complex than the relatively straightforward statement of penalties for violating the ITAR.[33] Generally speaking, the penalties assessed for violating the new regulations can be about as severe as those for violating the old regulations, with the exception that the maximum term of imprisonment is 5 years rather than 10 years.

EXAMPLES

Let's examine how the above regulations have been applied to certain popular cryptosystems. Collecting such examples is hampered by the fact that the government does not publish its decisions as to what particular cryptography is or is not exportable.

First, prior to December 1996, DES (Data Encryption Standard), although the subject of a domestic FIPS, *infra*, was generally not exportable except by banks and other financial institutions using DES to communicate with their foreign-based subsidiaries, and only with respect to the financial transactions themselves, not for any other types of communications. Recall that DES is a 56-bit symmetric cypher. The situation with respect to DES changed with the Commerce Department Regulations published in December 1996. Triple-DES cannot be legally exported.

Symmetric cyphers such as RC2 and RC4 are generally exportable as long as their key size does not exceed 40 bits. In August 1995, the Clinton Administration announced that these limits would be increased to 64 bits as long as the keys are left in government escrow. The Administration backtracked from this promise when the new Commerce Department Regulations were finally enacted in December 1996: said Regulations place the export-with-escrow threshold at 56 bits, not 64 bits.

Generally speaking, the government has been allowing licenses for the export of symmetric 56-bit encryption when the end user is a foreign subsidiary of a U.S. firm. However, this policy has been implemented on a case-by-case basis, and does not appear in any government regulations.

In January 1996, IBM won permission to export Lotus Notes 4.0 with a "differential work factor": the program presents 64 bits to potential code-breakers, but 40 bits to the U.S. government, even internationally.

Public key algorithms have been regulated on a functionality basis. For example, strong (greater than 512-bit) public key cryptography using the RSA algorithm was, prior to 1996, not normally allowed to be exported when used for encryption purposes.[34] However, 512-bit RSA is now allowed to be exported, but on a case-by-case basis; there is no mention of this in the Commerce Department Regulations. One company was allowed an export license when the encryption was limited to credit card numbers, and the keylength was limited to 1024 bits. The State Department set the limit at 512 bits when the function of the product was key management. When the function of the product was digital signatures, there was no restriction on key size, but a hash algorithm had to be used, so that the digital signature was applied to a message digest and not to the entire message. The new Commerce Regulations expressly permit 512 bits for the limited purpose of exchanging a session key.

PGP cannot normally be exported, but the commercial version of PGP, ViaCrypt, has been cleared for export for at least one U.S. company to communicate with its foreign subsidiaries.

The El Gamal elliptic curve algorithm has been regulated on a case-by-case basis.

For cryptography products that combine several cryptographic functions, the government deems the product to be exportable only if all of the cryptographic functions *independently* satisfy exportable criteria.

FEDERAL INFORMATION PROCESSING STANDARDS

Another important technique by which the U.S. government attempts to control cryptography is via Federal Information Processing Standards (FIPS). These documents, which are now issued by the National Institute of Standards and Technology (NIST), a branch of the Commerce Department, typically specify that certain cryptographic algorithms must be used for all government procurement. By this technique, the Executive Branch hopes to use economic pressure to thwart the use of non-favored algorithms.

The first major FIPS pertinent to cryptography was FIPS 46 on DES (Data Encryption Standard), issued in 1977. The DES algorithm has been published and studied widely. However, export restrictions apply to DES, as described above. Due to advances in computer science since 1977, DES's 56-bit keylength is no longer large enough to qualify DES as a truly strong algorithm. It has been reported that DES has been broken (cracked). As a result, many users are using the algorithm three times in succession in a technique known as triple-DES. There are rumors that even triple-DES has been cracked.

In part because DES was becoming technically obsolete, and because its published nature made it easy for DES to be widely copied and distributed throughout the world (despite the presence of export controls), the U.S. government issued, in February 1994, highly controversial FIPS 185 entitled EES (Escrowed Encryption Standard). The algorithm that is the heart of EES is called Skipjack, an 80-bit symmetric algorithm developed by the National Security Agency (NSA). Skipjack, unlike DES, is classified. This led to criticism that the algorithm could not be fully verified, and to suspicion that the NSA had embedded secret trapdoors in the algorithm. The widely publicized Clipper Chip portion of EES pertains to digital telephony, and contemplates the use of a hardware-implemented Skipjack algorithm along with associated circuitry, including a LEAF (Law Enforcement Access Field). The Capstone portion of the EES contemplates a chip combining the encryption functions of Clipper with DSA (Digital Signature Algorithm) for authentication and integrity purposes. EES also contemplates the Capstone Chip being available in a PCMCIA card now known as Fortezza.

The most controversial aspect of EES is that it is a government key escrow system. EES requires that one of the keys be split in two and held in escrow by two government custodians. This enables a government law enforcement agency (usually but not necessarily needing a court order) to obtain the keys from the escrow custodians, enabling the government to eavesdrop on the otherwise confidential communications. This provision engendered strong and vocal opposition from industry and civil liberties groups.

In an attempt to make the EES more palatable to industry, the government announced that products embodying the Skipjack algorithm would be exportable despite the fact that the Skipjack algorithm is classified. However, industry observers point out that a foreign user is not likely to purchase a cryptographic product in which the U.S. government has a back door through which it can enter and eavesdrop on confidential communications. Meanwhile, many Clipper Chip telephones have now been sold to the U.S. government, so the government has partially achieved its objective.

Because of the widespread industry aversion to the EES, the government is currently looking at other alternatives, including allowing commercial key escrow as long as the government has the ability to recover the keys.

Another objection that has been raised to the use of FIPS as legal instruments to control cryptography is that the government is using an obscure procedure originally intended to enable the National Bureau of Standards (the predecessor agency to NIST) to set standards for weights and measures, and that this procedure is inappropriate for the complex field of cryptography. It has been alleged that the Executive Branch has used this procedure for the purpose of bypassing Congress, in order to avoid the controversy that would break out if this issue were debated in Congress. In furtherance of its technique of bypassing Congress, the Executive Branch used its own funds, not requiring appropriations by Congress, to fund some of the initial purchases of telephones containing Clipper Chips. Critics have argued that it is precisely because the issue is so important and controversial that it should be debated in Congress.[35]

Soon after the EES FIPS 185 was issued, the NIST issued, in May 1994, FIPS 186 entitled Digital Signature Standard (DSS), making the Digital Signature Algorithm (DSA) a standard for authentication, including integrity. DSS is also an ANSI (American National Standards Institute) standard. DSA was developed by the National Security Agency (NSA), and is based on the El Gamal algorithm. Prior to the adoption of DSA as the basis for the FIPS on DSS, the U.S. government, in an unusual move, filed a patent application on DSA[36], in an attempt to lock everybody else out, with the intent to subsequently license its patent to all comers, thereby strengthening the position of DSA as a standard. This is an example of the government using the patent laws to control cryptography. It was then alleged by German inventor Claus Schnorr that DSA could not be practiced without infringing *his* digital signature patent[37] and two of the Stanford public key patents, *infra*.

Cryptographers have alleged that DSA is faulty in that it allows the government to forge digital signatures. Most of industry had tried to get the RSA algorithm to be the standard for digital signatures. The government preferred DSA, because DSA (unlike RSA) doesn't have encryption capabilities. This again shows the government's great sensitivity to cryptography having an encryption function. The government is not very concerned about cryptography having an authentication function.

Other FIPS relating to cryptography have been issued, such as FIPS 180 covering a Secure Hash Standard (SHS), issued in 1993. The secure hash algorithm covered by this standard is the message digest algorithm for the DSS, and was also developed by the NSA.

POLICY DEVELOPMENTS

There have been recurrent rumors that the government may venture beyond FIPS and export control laws, and pass laws that would mandate or prohibit certain types of cryptography within the United States for all purposes. Fueling this speculation was the disclosure of a classified memo authored by the FBI and other agencies in February 1993 recommending that only government-approved crypto should be allowed for use within the U.S.[38] FBI Director Louis Freeh asked for this in Congressional testimony following the bombing of the federal building in Oklahoma City in April 1995. Making this unlikely, however, is the First Amendment to the United States Constitution, the fact that strong encryption algorithms are widely available internationally, the existence of powerful commercial interests, and an increasingly informed and concerned citizenry. The dismissal of the Zimmermann investigation, the December 1996 Commerce Department regulations, and the April and December 1996 decisions in the *Bernstein* litigation, *infra*, show that the government is ever so gradually relaxing, or being forced to relax, its control of cryptography.

In January 1996, the U.S. Department of Commerce and the National Security Agency issued a partially classified report entitled "A Study of the International Market for Computer Software with Encryption" on behalf of the U.S. government's Interagency Working Group on Encryption and Telecommunications Policy. The study concluded that export restrictions on cryptography were indeed hurting United States firms vis-à-vis their foreign competitors. Specifically, the study reported that the U.S. market share of cryptographic products in Switzerland, Denmark, and the United Kingdom had declined because of U.S. export controls. The Commerce Department was expected to quickly forward a package of recommended reforms to the President. However, in March 1996, the Commerce Department announced that any such recommended reforms would be postponed. This was apparently due to internal pressure within the administration from the Federal Bureau of Investigation, which, as alluded to above, desires even stronger controls on cryptography than presently exist.

Also in January 1996, the Computer Systems Policy Project (CSPP) issued a white paper entitled "Perspectives on Security in the Information Age", concluding that U.S. export control policies severely limit the ability of United States companies to provide their customers with global security solutions based on encryption that are seamlessly integrated into their computer systems. The CSPP is comprised of the chief executive officers of many significant United States computer companies, including Apple Computer, AT&T, Compaq, Cray Research, Data General, Digital Equipment Corporation (DEC), Hewlett-Packard, IBM, Silicon Graphics, Stratus Computer, Sun Microsystems, Tandem, and UniSys. This CSPP report called for a number of reforms in the cryptography export policy. However, in the latter part of 1996, the CSPP began to split internally, with IBM and then DEC endorsing the government's plan for minor liberalization of the export control laws in return for a chance to develop government-approved government key recovery systems, which some corporations viewed as an opportunity to enhance revenues.

In May 1996, the prestigious National Academy of Sciences/National Research Council (NAS/NRC) issued a preliminary report on cryptography,[39] with the final report promised in 1997. Some of the findings in the NAS/NRC report are:

- current United States policy discourages the use of cryptography;
- the benefits of cryptography outweigh its disadvantages;
- cryptography can help law enforcement as well as hurt it;
- there should be no restrictions on the domestic use of cryptography;
- there should be a full national discussion on cryptography policy;
- the policy should be more aligned with market forces;
- jurisdiction over exporting 56-bit DES should be moved to the Commerce Department;
- the export process should be streamlined;
- approval for exports should be expedited for trustworthy companies; and
- authentication and public key infrastructure should be promoted.

LEGAL CHALLENGES TO EXPORT CONTROL REGIME

Despite the difficulty in mounting a legal challenge to the export control regime, for reasons alluded to above[40], there are several important cases, three of them current, which have done just that.

ZIMMERMANN CASE

The first case stemmed from the government's investigation of Phil Zimmermann, the inventor of PGP and the subject of a federal grand jury investigation that was convened in San Jose, California. The government conducted a 28-month investigation (from September 1993 until January 1996) as to whether Mr. Zimmermann made PGP encryption software available to U.S. citizens knowing they would freely post the software on the Internet, so that foreign nationals would have access to this software. The ITAR provides that making a defense article available to a foreign person in any manner constitutes an export, without specifically mentioning the Internet.

As an aside, it is noted that it has become increasingly common for persons to make software available via FTP (file transfer protocol) or for downloading from the World Wide Web segments of the Internet with warnings that foreign persons must not download the software. There had been doubt as to whether such warnings have any legal efficacy. This technique has never been tested in court. Prior to December 1996, the U.S. government had not issued any regulations or even guidelines on how to restrict foreign nationals from downloading sensitive materials off the Internet. In July 1996, the U.S. government gave permission to Netscape Communications to allow its U.S. customers to download a version of its software containing RC4 with a 128 bit keyspace off the Internet, provided measures were taken to prevent foreign nationals from doing so. In December 1996, the Commerce Department issued regulations on this topic, as mentioned earlier.

In January 1996, the government announced that it was dropping its investigation and would not indict Mr. Zimmermann. Despite that, the government's 28-month investigation sent a powerful message to those who would dare to challenge the government's regime of export control regulations. Perhaps ironically, in response to

the government's investigation of Zimmermann, a grass roots movement sprang up, creating a stronger force challenging said regime. This movement is embodied in the Internet Privacy Coalition (IPC), which had its first physical meeting in San Francisco in January 1997. The IPC is a coalition of several civil liberties groups.

KARN CASE

The second important case of interest had its origins in the request for Commodity Jurisdiction (CJ) made by Phil Karn, a cryptographer and engineer at Qualcomm, San Diego, California**.** Mr. Karn submitted two CJ requests, one for the export of Bruce Schneier's book *Applied Cryptography*, and a second for a software diskette containing cryptographic source code that was listed in the book. Rather surprisingly to most people, the State Department allowed export of the book[41] but not export of the software listed in the book[42]. Observers have said that this is tantamount to a law against typing, or a law against optical character scanning. One could refer to it as a McLuhanesque decision, as the State Department in essence held that the medium is the message.

The *Karn* case shows that the government places great credence in the distinction between technical data and software. This distinction is important not just in the ITAR, but also in government procurement regulations generally, as government contracts attorneys know.

Despite the above-mentioned impediments to mounting a court challenge against an adverse CJ determination, Mr. Karn filed a lawsuit in September 1995 seeking to overturn the State Department's adverse ruling. This case was assigned to Judge Charles Richey in the U.S. District Court for the District of Columbia. In March 1996, Judge Richey dismissed the case under the political question doctrine, stating that the issue was a policy decision within the purview of the Executive Branch.[43] Karn appealed. In January 1997, the Court of Appeals for the D.C. Circuit remanded the case back to the district court to take into account the new Commerce Department Regulations that were enacted in December 1996.

BERNSTEIN CASE

The third important legal case pertaining to the export of cryptography is the lawsuit filed in February 1995 by Daniel Bernstein against the U.S. Department of State, other agencies, and government officials.[44] The *Bernstein* case challenges the export control regime for cryptography on constitutional grounds — primarily the First Amendment's protection of freedom of speech — and is being supported by the Electronic Frontier Foundation (EFF). In October 1995, Judge Marilyn Hall Patel of the U.S. District Court for the Northern District of California heard the government's motion for summary judgment to dismiss. In April 1996, Judge Patel denied the government's motion in a pathbreaking opinion holding that computer source code is speech for purposes of the First Amendment.[45] This was the first time a court had so held.

Bernstein then filed a summary judgment motion to invalidate the entire ITAR scheme for cryptography. In support of this motion, Bernstein's attorneys filed a powerful and well-supported memorandum asserting that said scheme is an impermissible

prior restraint of freedom of speech, impermissibly restricts the content of speech, is unconstitutionally vague, and is unconstitutionally overbroad. Bernstein's attorneys submitted evidence that strong encryption is overwhelmingly used for peaceful, not criminal, purposes; and has been used by human rights organizations in the Balkans, Burma, Guatemala, and Tibet to protect the lives of people struggling against totalitarian regimes.

In December 1996, Judge Patel took the next logical step and declared the entire ITAR scheme of controlling crypto exports to be unconstitutional under the First Amendment. The *Bernstein* case is now being expanded in scope to consider the new Commerce Department regulations that were announced just days after Judge Patel's December 1996 decision. It is likely that the *Bernstein* case and/or the *Karn* case will ultimately be decided by the U.S. Supreme Court.

In the *Bernstein* case, the government went even further than it did in the *Karn* case in attempting to regulate cryptography: the State Department had sent a letter to Bernstein advising him that he must first obtain a license from the State Department before he could publish a scientific paper describing his cryptographic algorithm[46]. Some two years later, after Bernstein had filed his lawsuit, the State Department withdrew its finding that publication of the paper would require a State Department license. The government was no doubt worried that the court would strike down this prohibition as a prior restraint on the freedom of speech guaranteed by the U.S. Constitution. This was indeed inevitable, given the court's December 1996 opinion.

JUNGER CASE

A fourth case that is challenging the government's cryptography export regulations is that of *Junger v. Christopher et al.*[47] filed in Federal District Court for the Northern District of Ohio by Peter D. Junger, a long term law professor at Case Western Reserve University Law School. The defendants are former Secretary of State Warren Christopher, the Director of the Office of Defense Trade Controls within the State Department, and the Director of the National Security Agency. In his complaint, Professor Junger alleges that he has been chilled by the government's laws and policies into not allowing foreign nationals to attend the law school class he teaches on computer law. This class discusses cryptographic information, most of which is taken from public sources, including materials published in books, journals, and on the Internet.

The cases described in this section are helping to force a liberalization of the crypto export laws, by focusing political as well as legal opposition to the government's policies.

PROPOSED LEGISLATION

In March 1996, Representative Goodlatte (R-VA) introduced H.R.3011, known as the Security And Freedom through Encryption (SAFE) Act. A companion bill was introduced the same day in the U.S. Senate by Senator Leahy (D-VT): S.1587, known as the Encrypted Communications Privacy Act of 1996. H.R.3011 was the subject of hearings before the House Judiciary Committee in September 1996.

Senator Leahy's bill was *de facto* withdrawn in favor of a subsequent Senate bill, S.1726, introduced by Senator Burns (R-MT) in May 1996, entitled Promotion of Commerce On-line in the Digital Era (Pro-CODE) Act of 1996. The full Senate Commerce Committee held hearings on Senator Burns' bill in July 1996. A scheduled September 1996 Senate vote on the bill was canceled. Both this Pro-CODE bill in the Senate and the SAFE Act in the House of Representatives are being re-introduced in 1997. Support seems to be gradually increasing for both bills.

The Goodlatte bill and the Burns bill both: 1) prohibit mandatory key escrow; 2) relax export controls for cryptographic products that are generally available in the public domain or have similar capability as ones currently permitted for export by financial institutions (financial institutions such as banks are currently given more leeway to export cryptographic products than other entities); and 3) allow the government the right to recover the keys for legitimate law enforcement purposes. Additionally, the Goodlatte bill provides for increased criminal penalties in cases where cryptography is used in the commission of a crime.

It is interesting to note that before he left the United States Senate to run for the Presidency, Senator Dole (R-KS) co-sponsored both the Leahy bill and the Burns bill, thus placing himself in direct opposition to the Clinton Administration on the issue of cryptography policy. Cryptography was not a major issue in the 1996 Presidential campaign, however.

INTERNATIONAL LAWS

One engaging in international commerce needs to be aware of the laws of each individual country in which one wishes to market one's product. Many countries restrict *import into* and *use of* cryptographic products within their boundaries (For example, France restricts import; while France, China, Belgium, and Russia all restrict use. In France, PGP is illegal; and the government has the right to eavesdrop when people exchange encrypted messages. On the other hand, Finland, South Africa, and Anguilla have no restrictions on cryptography at all, or else the regulations in effect are not enforced. Generally speaking, no other country regulates the *export* of cryptography as strictly as does the United States.

The U.S. government has been attempting to promote its proposals for government key recovery on the international level. The principal international forum for this has been the Organization for Economic Cooperation and Development (OECD) based in Paris. The choice of the OECD is somewhat surprising, given the fact that the OECD, unlike its sister organizations such as the United Nations, International Monetary Fund, World Bank, and World Trade Organization, has no enforcement powers. It is simply a forum for arriving, via secret deliberations, at policy positions on important economic issues involving the world's major countries. The OECD has been jealous of its role. When UNESCO, a specialized agency of the United Nations, requested that it sit in on the secret OECD cryptography meetings as an observer, OECD queried UNESCO as to why it thought it had a right to be there. It has been suggested that the U.S. government selected the OECD as the forum for international crypto policy precisely because deliberations within the OECD are secret.

The United States has made some headway in getting other countries, e.g., the United Kingdom, to endorse its government key recovery proposals. On the other hand, some countries, such as Denmark, have taken a more civil libertarian position. The Netherlands opposed the U.S. in the OECD on the question of government key recovery.

Japan's encryption policies have historically been shaped almost exclusively by commercial interests. The export of crypto out of Japan is controlled on a case by case basis, but keylength is not a factor. The Japanese government actively encourages the use of cryptography, making it voluntary and market driven. It is interesting to note that the Japanese constitution prohibits the use of wiretapping, although the government occasionally engages in this practice following a court order. In the OECD, Japan started out with a civil libertarian position, but, after being pressured by the U.S., has recently indicated that it might be willing to consider key escrow proposals. Japan is an important country in this debate, because some of its companies, such as NTT (Nippon Telephone and Telegraph) have started to introduce products that will challenge the current large lead enjoyed by American companies in the field of cryptography.

In November 1996, the U.S.'s representative to the OECD talks, David Aaron, was elevated to the rank of Ambassador, giving an indication of the importance with which the Administration views the issue. The principal crypto policy maker in the United States, however, appears to be Vice President Gore. The government also has an Interagency Working Group on Encryption and Telecommunications.[48]

At the January 1997 RSA Data Security Conference, Ambassador Aaron stated that the OECD delegates subscribed to the U.S. desire for government key recovery, and that many countries want stronger controls on cryptography than does the United States. Both of these assertions were vigorously disputed by Marc Rotenberg, Director of the Electronic Privacy Information Center (EPIC), who has attended most of the OECD crypto meetings.

In March 1996, the European Commission adopted a Green Paper which stated that the absence of harmonized rules for the legal protection of encrypted services is preventing the proper functioning and development of Europe's single market in this sector.

INDUSTRY AND NON-U.S. GOVERNMENT STANDARDS

One entering the cryptography market must also be cognizant of standards for cryptography that are under development by various non-governmental, quasi-governmental, and non-U.S.-based groups, such as the IEEE (Institute of Electrical and Electronic Engineers), ANSI (American National Standards Institute) Internet IEFT, World Wide Web Consortium (W3C), ISO (International Standards Organization), and CCITT (Consultative Committee for International Telegraphy and Telephony).

While not having the force of law when promulgated by an industry group, such standards are influential in shaping industry practice and in facilitating market acceptance.

Specifically, the Internet PEM (Privacy Enhanced Mail) Standard, IETF PKIX, ISO/IEC/CCITT-X.509 (pertaining to the structure of digital certificates), ANSI X9.55, S/MIME (Secure Multipurpose Internet Mail Extensions), S/WAN (Secure Wide Area Networks), PKCS (Public Key Cryptography Standards), Cryptoki (Cryptographic Token Interface), France's ETEBAC 5, and Australia's AS 2805.6.5.3 should be watched as they evolve and are implemented. Also of interest are ISO/IEC 9798.5 pertaining to authentication, ISO/IEC 9796.2 pertaining to digital signatures, and ISO/IEC 7816.4 pertaining to secure messaging.

In February 1996, Visa International and Master Card International jointly announced a new technical standard, Secure Electronic Transactions (SET), for safeguarding credit card purchases made over open networks, most particularly including the Internet. The two companies had been pursuing separate standards. The new standard, which used cryptography developed by RSA Data Security, Inc., should make it easier to exchange credit card numbers over open networks, and thereby facilitate on-line commerce.

PATENT ISSUES

Another legal issue facing those in the cryptography business has been the question of patents relating to cryptography. Some early patent applications covering cryptosystems were placed under Secrecy Orders by intervention of the NSA under the authority of the Invention Secrecy Act of 1940 and the National Security Act of 1947. However, hundreds of other cryptography patents have issued in the United States. Important among this group has been a patent,[49] owned by the Massachusetts Institute of Technology (MIT) and exclusively licensed to RSA Data Security, Inc., covering the first successful implementation of public key cryptography. This invention was made by Drs. Rivest, Shamir, and Adleman. Also important have been three Stanford-owned patents covering public key cryptography. These patents were exclusively licensed to Cylink Corporation, and are known as the Diffie-Hellman[50], Hellman-Pohlig[51], and Hellman-Merkle[52] patents. PGP (Pretty Good Privacy) is licensed under the MIT patent and the Hellman-Merkle patent.

In 1990, RSA Data Security, Inc. and Cylink Corporation formed a partnership called PKP (Public Key Partners) to pool these patents and license them to the nascent field of public key cryptography companies. However, differences subsequently arose between RSA and Cylink; and PKP was ordered dissolved by an arbitration panel in 1995.

PRE-RSA/CYLINK PATENT LITIGATION

The Hellman-Pohlig patent was in an "interference" with the MIT patent. An interference is a quasi-judicial proceeding within the U.S. Patent and Trademark Office to determine the first and true inventor when there are two or more contenders. This interference was settled between the applicants.

In the mid-1980's, RSA sued mathematician Roger Schlafly and his partner Digital Signature over his Cryptmaster software. Under a 1988 consent decree, Schlafly agreed to cease production of his product.

In 1992, PKP sued TRW for infringing one of Stanford's patents over TRW's use of the El Gamal public key cryptosystem. That suit settled in June 1992 with TRW agreeing to take a license.

In 1993, Roger Schlafly sued NIST (National Institute of Standards and Technology) to prevent NIST from licensing DSA (NIST's Digital Signature Algorithm standard, *supra*) through PKP. That suit was dismissed.

In 1994, Roger Schlafly filed suit against PKP and RSA in U.S. District Court for the Northern Court of California alleging, among other things, that the MIT patent and two of the Stanford patents are invalid.[53] PKP had asserted that Schlafly improperly used PKP's patents in Schlafly's work for AT&T's Secret Agent cryptosystem. This suit remains pending, despite the fact that PKP has been dissolved, *infra*.

RSA/CYLINK PATENT LITIGATION

The mid-1990's witnessed a series of bitter patent lawsuits between RSA Data Security, Inc. and Cylink Corporation. First, RSA sued Cylink in California Superior Court for the County of Santa Clara in 1994[54] to try to resolve some of the licensing questions that had beset the parties. In 1995, under the auspices of this state court, an arbitration panel ordered that PKP be dissolved.

Next, in June 1994, Cylink brought a lawsuit in U.S. District Court for the Northern District Court of California alleging that the MIT patent is invalid.[55] MIT became a third party intervenor in this lawsuit in January 1995. MIT and RSA took the firm position in this lawsuit that the MIT patent is valid. This position has never been judicially impugned. This case was eventually assigned to Judge Letts sitting by designation from the Central District of California.

In a third lawsuit, after Cylink had contacted some of RSA's customers, asserting that these customers needed licenses under the Stanford patents before these customers could practice the invention covered by the MIT patent, RSA sued Cylink and Stanford in September 1995 in U.S. District Court for the Northern District of California, alleging that the three Stanford patents are invalid.[56] This case was partially consolidated by Judge Spencer Williams with the case of *Schlafly v. Public Key Partners et al., supra*.

Finally, in a fourth lawsuit, Cylink sued Dr. Schnorr and RSA in November 1995 in U.S. District Court for the District of Columbia, seeking a declaratory judgment that the practice of the Digital Signature Algorithm (DSA) in complying with the Federal Information Processing Standard on the DSS (discussed previously) does not infringe Dr. Schnorr's patent.[57] RSA Data Security, representing Dr. Schnorr with respect to licensing this patent, had previously requested that Cylink cease using DSS in its products without a license to the Schnorr patent. In September 1996, the district court dismissed the case. Cylink appealed to the United States Court of Appeals for the Federal Circuit.[58]

All four of these lawsuits were settled in December 1996 by means of RSA and Cylink cross-licensing each other on the patents for which they are the exclusive first-tier licensee.

[1] C. 1953, 46-3-101 et seq., enacted by Laws 1995, ch. 61.

[2] Froomkin, "The Essential Role of Trusted Third Parties in Electronic Commerce," 75 *Oregon L. Rev.* 49 (1996).

[3] Gov. Code §16.5, added by Stats. 1995, c.28 (A.B. 1247), §1.7.

[4] "New Directions in Cryptography", *IEEE Transactions on Information Theory*, Nov. 1976. The first sentence of that paper was prophetic: "We stand today on the brink of a revolution in cryptography."

[5] U.S. patent 4,405,829.

[6] In April 1996, RSA Data Security, Inc. was acquired by Security Dynamics Technologies of Cambridge, Massachusetts.

[7] A message digest is sometimes called a one-way hash.

[8] 22 C.F.R. §§ 120-130, as amended by 58 Fed. Reg. 39,280 (1995).

[9] 22 U.S.C. § 2778.

[10] The NSA is a separately organized agency within the Department of Defense.

[11] Section 120.11.

[12] Section 120.10.

[13] Section 120.10.

[14] 10 F.3d 808 (9th Cir. 1993) (unpublished disposition).

[15] 904 F.2d 601 (11th Cir. 1990).

[16] 22 U.S.C. § 2778(c).

[17] Federal Register, Vol. 6l, No. 33; 61 FR 6111, February 16, 1996.

[18] The prohibition on demonstration of the product abroad was relaxed in the December 1996 Commerce Department Regulations.

[19] 57 Fed. Reg. 32,148 (1992), amending 22 C.F.R. § 121.1, Category XIII(b)(1).

[20] Rubenstein, "Export Controls on Encryption Software," October 17, 1994, in *Coping with U.S. Export Controls 1994* (PLI Com. Law & Practice Course Handbook Series No. A-705), citing a 1989 joint Commerce/State Department unpublished memo.

[21] 22 CFR § 120.4(g).

[22] 22 U.S.C. § 2778 (h).

[23] 579 F.2d 516 (9th Cir. 1978).

[24] Executive Order 13026 of Nov. 15, 1996, 61 Federal Register 58,767 (Nov. 19, 1996).

[25] 61 Federal Register 241, Dec. 13, 1996. These regulations provide, *inter alia*, that one normally must be a U.S. citizen in order to become a key recovery agent.

[26] "Encryption Items Transferred From the U.S. Munitions List to the Commerce Control List", 61 Federal Register 68572, Dec. 30, 1996.

[27] 5 U.S.C. 553.

[28] 15 CFR §734.2(b)(9)(B)(ii).

[29] *New York Times v. United States*, 403 U.S. 713 (1971), commonly referred to as the Pentagon Papers case.

[30] *Rubenstein, supra*, at pp. 213-214.

[31] Patricia Jackson, personal communication, February 1997.

[32] 15 CFR §742(b)(3)(v)(E)(2).

[33] 50 U.S.C. APP. §2410; 50 U.S.C. APP. §2411(a)(5)(1996).

[34] The keyspace of an asymmetric cypher is greater than the keyspace of a symmetric cypher of comparable strength.

[35] Froomkin, "The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution", 143 *University of Pennsylvania Law Review* 709-897 (1995).

[36] The inventor is David Kravitz.

[37] U.S. patent 4,995,082.

[38] In a briefing document entitled "Encryption: The Threat, Applications, and Potential Solutions," sent to the National Security Council in February 1993, the FBI, NSA, and Department of Justice stated: "...technical solutions, such as they are, will only work if they are incorporated into all encryption products. To ensure that this occurs, legislation mandating the use of government-approved encryption products or adherence to government encryption criteria is required."

[39] *Cryptography's Role in Securing the Information Society*.

[40] See the section entitled "Administrative and Judicial Appeals".

[41] CJ Case 038-94.

[42] CJ Case 081-94.

[43] *Karn v. U.S. Department of State*, 925 F.Supp. 1 (D.D.C. 1996).

[44] *Bernstein v. U.S. Department of State*, Civil Action No. C95-0582-MHP (N.D. Calif.).

[45] 922 F.Supp. 1426 (N.D. Cal. 1996).

[46] Snuffle 5.0.

[47] Case No. 1:96 CV 1723.

[48] This Group is currently co-chaired by Ed Appel and Mike Nelson.

[49] U.S. patent 4,405,829.

[50] U.S. patent 4,200,770.

[51] U.S. patent 4,424,414.

[52] U.S. patent 4,218,582.

[53] *Schlafly v. Public Key Partners, et al.*, No. C-94-20512 SW.

[54] No. CV-740794.

[55] *Cylink Corp. v. RSA Data Security, Inc., et al.*, No. C-94-2332 JSL.

[56] *RSA Data Security, Inc. v. Cylink Corp. et al.*, No. C-95-3256 SW.

[57] U.S. patent 4,995,082.

[58] No. 97-1109.