© Abrams/Zacagnina/The Image Bank

Protecting Privacy in the Cyber Era

Jennifer C. Davis

Almost daily we are asked, or required, to fill out forms with personal information — credit applications, questionnaires, service contracts, insurance forms, medical treatment forms, driver's license applications, and the list goes on. All of this information is collected into databases. Once in the database, the information is studied and manipulated. Public policy and tactical business decisions often rely upon trends uncovered by statistical analysis of these data. Personal information is also used to make crucial decisions about individuals — who will get a job, mortgage, or credit card. However, when information in a database is personal — or "nonstatistical" (can be connected to an individual), the potential for its misuse can be staggering.

As a society, we have determined that certain private information should be protected. A credit agency, for example, does not have the right under U.S. law to require people applying for credit to inform the agency of their race and marital status [1]. If, however, the agency has done studies that indicate that single people, for example, are more likely to default on interest payments than married people, it has an interest in somehow obtaining this information. It turns out that obtaining this type of data is very easy, as marriage licenses are public records, and as such, are accessible through online information services like Lexis-Nexis. If the credit agency directors really think that it is in the

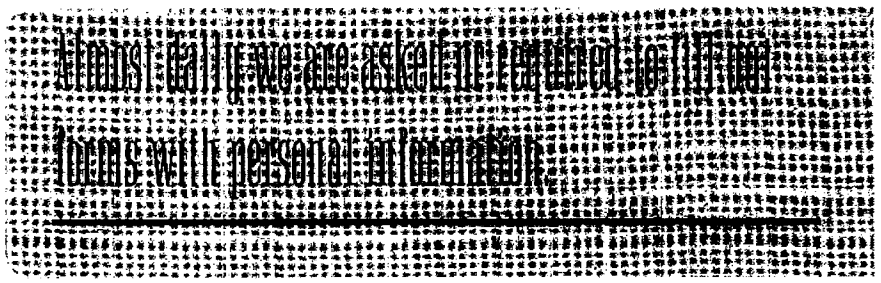
The author was at Princeton University, Princeton, NJ. She is now with SciTec, Inc., 100 Wall St., Princeton, NJ 08540; email: jdavis@scitec.com.

0278-0079/00/$10.00©2000IEEE

company's best interest to find out the marital status of each and every applicant, they can simply access the Lexis-Nexis databases, type in the applicant's name and other identifying information, and wait for data to appear on their computer screens.

Not only is a great deal of personal information freely available to any who care to go searching for it, but often security measures that are put in place to protect sensitive data are ineffective — either inherently (hackers can easily crack the codes), or simply because authorized users of the data illegally pass it on to outsiders. This lack of security surrounding private information has lately been the subject of numerous headlines. For instance, a United States Naval officer recently initiated legal action against the Navy for dismissing him when they found out that he was gay [2]. Having abided by the military's "don't ask, don't tell" policy, officer Timothy R. McVeigh claimed that he had been wrongfully dismissed, as he had not told anyone in the Navy about his sexual orientation. McVeigh soon discovered that prior to dismissing him, the Navy had acquired information on McVeigh's sexual orientation under false pretenses from McVeigh's on-line service supplier, America On-Line (AOL). According to Title II of the 1986 Electronic Communications Privacy Act [3], it is illegal for on-line services to disclose personal information without a warrant.

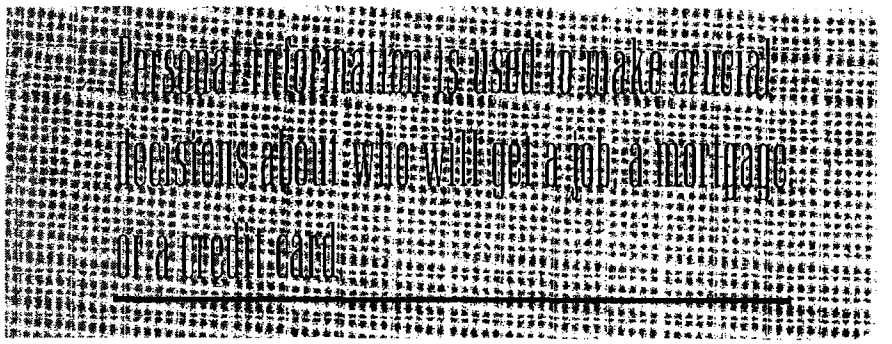
Controversy has surrounded numerous other databases as well. After cases such as the O.J. Simpson murder trial, almost everyone knows about the use of DNA tests by law enforcement agencies to tie suspects to crime scenes. DNA sequences from a diverse variety of tissue samples can be analyzed and matched (to within a calculated uncertainty) to corresponding DNA sequences from other samples. Large DNA databases are required to support sample matching and statistical analyses. In order to facilitate the matching process, some states routinely collect DNA samples from convicted felons.



Other government agencies have expressed interest in harnessing DNA data for their own use. Currently, the Department of Defense (DoD) proposes building a mammoth DNA database comprised of DNA records from all current and former military and reserve soldiers. The motivation for this database, DoD claims, is to be able to identify recovered bodies of servicemen. According to Banisar in his article, "Big Brother is watching," however, "two soldiers have filed suit to prevent the collection of their genetic information arguing that it is an invasion of privacy and that there are no restrictions on how the DNA can be used" [4]. It is understandable that soldiers worry about their genetic maps resting in files that are accessible by countless people unknown to them. After all, a person's DNA represents a comprehensive blueprint of his or her physical being. It can be argued that criminals cede some of their rights to privacy when they commit acts that break the law. Thus, coerced collection of their genetic information is acceptable to most people. The collection of DNA samples from military personnel, however, constitutes an invasion of privacy that is unacceptable to some. The possibilities for the misuse of such a DNA database outweigh its potential benefits for the soldiers filing suit.

Perhaps one reason that the collection of DNA or other biometric data is so unnerving is that often just about anyone can buy access to equally personal information, despite assurances that these data are protected. On the Internet, many companies flourish selling their ability to access (legally or, sometimes, illegally) databases filled with personal data. These companies, called 'information brokers,' can uncover almost any kind of information about a person or business entity for a price. For example, a person's bank balance can be provided for $190, his or her salary for $75, credit card number for $450, or medical history for $400 [5]. Jason Rowe, a private investigator quoted in a *New York Times* article on "High-tech sleuths," claims that "everything you want to know is for sale. It's a question of how much risk you want to take and what your personal morals are" [6].

Often privacy is also intruded upon directly, via tapping of telephone lines or monitoring of cellular telephone conversations transmitted via satellite on radio waves. One very publicized case illustrating the lack of security in early cellular phone communications involves Great Britain's Prince Charles. All over the world, very embarrassing cellular phone conversations between Prince Charles and Camilla Parker Bowles were made public, much to the chagrin of the Royal Family. The privacy of data transmitted over telephone or electric wires, fiber optic cables, or via satellite is also vulnerable. Clearly, there is a need to protect the data transmitted in financial trans-



actions such as the personal identification numbers (PINs) used by millions of people to extract cash at automatic teller machines, or any sort of code that provides access to bank accounts or credit lines. Especially now that business transactions are being performed over the 'lawless' Internet, it is crucial that dependable security be provided for these important data transmissions.

Protecting Privacy in the Cyber Era

Measures providing privacy protection to citizens have been, and are currently being, implemented at various levels in our society. In the U.S. political arena, all three branches of government, executive, legislative, and judicial, have played a part in defining the role of privacy in American society. Industry and concerned private citizens have also helped to shape privacy issues by initiating public debate and by developing solutions for securing private communications and data. Often the different stakeholders have found themselves at odds with one another over the issues: To what extent is the protection of an individual's or a business' privacy more important than securing potential law enforcement or national security interests? What are, exactly, a person's legal rights to privacy?

From our beginnings as a nation, the protection of privacy, mainly in the form of private property and speech, has been an important goal of our laws. First and foremost of these laws are the First, Fourth, and Fifth Amendments of the U.S. Constitution, which pertain to the rights of American people to be protected from certain invasions of their privacy. The First Amendment protects our free speech, free press, and free assembly; The Fourth Amendment sets limits for legally sanctioned searches of private homes and personal effects; and under the Fifth Amendment, "[n]o person. . . shall be compelled in any criminal case to be a witness against himself" (U.S. Constitution, Amend. V, quoted in [7]). In addition to the broad, sweeping protections afforded by the Constitution, numerous other laws have been enacted in order to further define the boundaries of personal privacy. It should be noted that protecting privacy in the sense that privacy is a "state or condition of limited access to a person"[8] is certainly not explicitly delineated in the Constitution. It is widely acknowledged that Warren and Brandeis' article on privacy, written in 1890 [9], brought the issue of privacy into public awareness. It is therefore somewhat astonishing that the Constitution, written before privacy really became an issue, can be used today in its defense (a good exposition on the extraction of privacy protection from the Constitution via U.S. case law can be found in the concurring opinion in *Griswold, et al. v. Connecticut*, 381 U.S. 479 (1965), written by Justice Goldberg).

As the collection of data has become simpler and swifter than ever before, thereby making it easier for the government to require us to divulge more and more information about ourselves in the interest of maintaining a smoothly running bureaucracy, many of the laws focusing on privacy protection have concerned securing, and limiting, the access to these data in government databanks. Whereas some of the legislation covering government data collection applies generally to all agencies, other privacy laws specifically regulate particular agencies.

According to the authors of the report on the status of privacy in America's government agencies ("the database study"), *Private Lives and Public Policies* [10], the most important government-wide privacy legislation includes: the Privacy Act of 1974 (5 U.S.C.S. 552a); the Freedom of Information Act of 1966 (5 U.S.C.S. 552); and the Computer Matching and Privacy Protection Act of 1988 (5 U.S.C.S. 552a).

- **Privacy Act:** The general provisions of this Act require that federal agencies 1) grant individuals access to their identifiable records that are maintained by the agency; 2) ensure that existing information is accurate and timely and limit the collection of unnecessary information; and 3) limit the disclosure of identifiable information to third parties. Civil and criminal penalties are delineated for failure to abide by the provisions outlined in the Act. One of the shortcomings of this Act, according to the authors of the database study, is that it does not protect statistical records from improper disclosure for non-research purposes [10].

- **Freedom of Information Act:** This law, like the Privacy Act, also "regulates the disclosure of research and statistical records"

[10]. More specifically, the Act "permits public access to records maintained by federal agencies unless the request for access falls within one of nine specific exemptions" [10]. By setting down rules for allowing public access to the databanks compiled using government resources, the individual's right to keep his or her personal information private is balanced against society's right to use the compiled information. In general, an attempt is made in these laws to restrict public access to individually identifiable information on the one hand, while allowing some access to statistical data on the other.

• **Computer Matching and Privacy Protection Act :** This act "regulates the use of computer matching of federal records subject to the Privacy Act". According to the authors of the database study, however, "[m]atches performed for statistical purposes are specifically excluded from the coverage of the act" [10].

The laws outlined above apply to all federal agencies. Often, however, agencies dealing with particularly sensitive data are regulated by legislation that is specific to their operation. The records maintained by the Bureau of the Census, for example, are stringently regulated under Title 13 of the United States Code (U.S.C.). Under this legislation, it is very difficult for anyone who is not a Census Bureau employee (and thus sworn to uphold the confidentiality provisions of Title 13) to gain access to individually identifiable Census data — even if these data are to be used only in statistical analyses. Similar restrictions are contained in Public Law 100-297, the Augustus F. Hawkins-Robert T. Stafford Elementary and Secondary School Improvement Amendment of the General Education Provision Act (GEPA), governing the data collected by the National Center for Education Statistics (NCES).

In general, the authors of the database study found that the current mishmash of privacy protection laws in the U.S. is not adequate. In their words, the "[c]urrent legislation impedes the constructive exchange of data for statistical and research purposes while failing to provide adequate protection of the confidentiality of statistical and research records" [11]. Furthermore, the authors specified two major inadequacies in the current legislation in the U.S. First, many agencies are not covered by confidentiality legislation that is tailored exclusively for protecting its data. Thus, these agencies must rely solely on the (inadequate) Privacy Act to protect an individual's identifiable information. Second, the extent to which various statistical agencies are covered by legislated confidentiality protection is extremely inconsistent. Therefore, the treatment of similar types of data varies from agency to agency, irrespective of the data's sensitivity.

In addition to laws governing the disposition of data collected by government agencies, legislation has been proposed, and sometimes passed, that protects privacy in other ways. The Electronic Communications Privacy Act of 1986 (P.L. 99-508) [3], for example, as outlined in its abstract, "[a]mends the Federal criminal code to extend the prohibition against the unauthorized interception of communications to specified types of electronic communications. Prohibits unauthorized access to an electronic communications system in order to obtain or alter information contained in such system. Prohibits the installation or use of a pen register or tracking device without a court order" (P.L. 99-508 abstract)[3]. Because the Navy violated the provisions of this Act when it queried AOL about the sexual orientation of Chief Petty Officer Timothy R. McVeigh (information that the Navy then used as the basis for dismissing him), McVeigh was able to successfully fight his dismissal in court [2].

There are numerous bills still pending in Congress that concern privacy protection. Some of these include:

• **Individual Privacy Protection Act of 1995 (H.R. 184)** [12]. This bill, introduced in the 104th congress by Rep. Collins of Illinois, was intended to "amend the privacy provisions of Title 5, United States Code, to improve protection of individual information and to reestablish a permanent Privacy Protection Commission as an independent entity in the Federal Government" (Text, as introduced in the House) [13]. The main purpose of this bill is to establish a commission whose specific assignment includes: studying databanks (both in the government and private sectors) in order to assess the confidentiality of private information kept therein; making recommendations to Congress and the President on the basis of these investigations; developing guidelines for the implementation of confidentiality legislation; investigating compliance with this legislation; reviewing Federal law, Executive orders, regulations, directions, and judicial decisions for consistency with regard to privacy rights; and finally, to commenting upon how proposed laws might affect privacy rights. It seems likely that this type of commission could perhaps have a positive influence on standardizing the confidentiality requirements protecting individual information in databases. Unfortunately, this bill has not been passed into law.

• **Encrypted Communications Privacy Act of 1997 (S. 376)** [11]. This bill was introduced during the 105th Congress by Sen. Leahy of Vermont on February 27, 1997. To privacy advocates, the most important of this bill's provisions are: 1) its affirmation that U.S. citizens are free to use any type of encryp-

tion in order to protect their personal data or communications, regardless of the encryption algorithm, key length, or implementation chosen, and 2) its prohibition against the government's requiring that as a condition of sale, an encryption key be held in escrow by a third party. Currently there is a great deal of heated debate between privacy advocates and certain law enforcement/national security factions over the issues of mandatory 'key escrow' encryption systems and the regulation of the exportation of encryption devices. There are presently, in fact, several bills being debated in Congress concerning these issues. As these bills, by and large, are predominantly regulatory — i.e., they are written in order to *limit* the use of encryption devices, as opposed to stressing an individual's right to use them, these bills will be discussed in a later section. In any case, due to the persuasiveness of the arguments of the law enforcement/national security faction (embodied by Louis B. Freeh, the director of the Federal Bureau of Investigation (FBI)), this bill is "dead in the water," according to reporter Ashley Dunn of *The New York Times* [13].

• **Communications Privacy and Consumer Empowerment Act (H.R. 1964)** [14]. Introduced June 19, 1997, by Representative Markey in the 105th Congress, the goal of this bill is to "protect consumer privacy, empower parents, enhance the telecommunications infrastructure for efficient electronic commerce, and safeguard data security" (text, H.R. 1964) [14]. The main privacy protection provisions contained in this proposed legislation include:

i) The requirement that the Federal Trade Commission (FTC) commence a proceeding to: 1) "determine the methods by which consumers may be enabled to have knowledge that consumer information is being collected about them, used without authorization, or sold through their utilization of telecommunications services and to exercise control over, and stop unauthorized use of, personal information;" and 2) "propose changes in FTC regulations and recommend legislative changes to correct defects in privacy rights and remedies of parents and consumers generally" (text - summary, H.R. 1964) and

ii) A prohibition barring the Federal Government or State governments from: "(1) restricting or regulating the sale in interstate commerce of encryption or other products for improvement of data security; (2) conditioning the issuance of certificates of authentication or authority upon any escrowing or sharing of private encryption keys; or (3) establishing a licensing or other regulatory scheme that requires key escrow as a condition of regulatory approval" (text - summary, H.R. 1964) [14]. Once again, it is unlikely that this bill will ever be passed into law.

Not only are the national security faction's arguments in favor of key escrow and regulating the sale of encryption devices likely to stall the passage of this bill, but a recent industry initiative concerning protecting the privacy of consumer information will very likely forestall any legislative action on the collection of consumer information issue. There are currently more than 80 bills that have been introduced in Congress similarly aimed at regulating the collection of, and the public's access to, personal data [15].

In 1996, Lexis-Nexis launched a controversial new service called "P-Trak", in which Social Security numbers and dates of birth were made available to the general public over the Internet. The appearance of this service spawned an uproar not only in privacy advocacy groups, but in the general public as well (and thus in political circles). In December 1997, in a move calculated to stem the resulting public outcry and to head off the passage into law of proposed restrictive legislation, fourteen information service companies including Lexis-Nexis, together controlling 90% of the on-line traffic in personal information, voluntarily agreed to limit the public's access to personal information. Although each of these companies agreed to limit the public's access to the databanks of personal information it maintains, complete access will still be granted to law enforcement agencies, banks, law firms, and other businesses. The "look-up" service companies will, however, bear the responsibility of determining whether or not potential clients have legitimate claims on their services. Another aspect of the agreement is that the data access limitations do not apply to information that is on public record. This type of data includes all information that is found in court documents and in marriage and divorce papers. Individuals are, however, given a chance to opt out of being a part of the companies' (publicly accessible) databanks in this agreement. If a person so desires, he or she must contact each of the companies and request that his or her information be removed. Finally, if one of the fourteen companies defies any of the terms of the pledge, it becomes vulnerable to prosecution by the states for engaging in deceptive practices. In alphabetical order, the fourteen companies signing the agreement are: Acxiom Corp., CDB Infotek, DCS Information Systems, Database Technologies Inc., Equifax Credit Information Services Inc., Experian, First Data Solutions Inc., Information America Inc., IRSC Inc., Lexis-Nexis, Metromail Corp., National Fraud Center, Online Professional Electronic Network, and Trans Union Corp [15].

Although the FTC endorses the

agreement, as does the Clinton Administration, which has stated that it would prefer not to resort to generating new laws and regulations to protect privacy in the Internet era [16], many civil libertarians fear that the agreement does not go far enough in protecting privacy rights. One of the concerns of the privacy groups is that under the terms of the pact, average citizens will not gain any new access to their own personal records so that they might check them for accuracy, nor can they find out what, or to whom, information about themselves is being sold. Another concern is that no remedies are offered to people who feel that they have been harmed by the companies' dissemination of their personal information. In Europe, relatively strong privacy legislation based on the European Data Protection Directive [17] is starting to go into effect. The European Data Protection Directive was implemented by Member States and specifically addresses many of the concerns raised by privacy groups, such as the data subject's access to the data and their rights regarding the disposition of their personal information. It looks as though this European privacy legislation might just be the coherent comprehensive system of privacy protection advocated by the National Research Council database study.

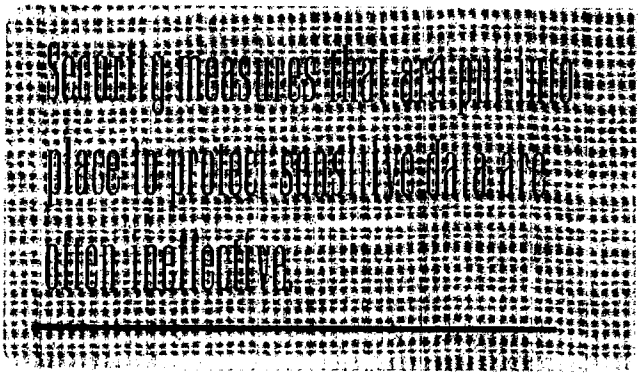
Despite the need for laws, regulations, executive orders, and industry pacts to help society define what is and what is not to be kept private and to determine guidelines for protecting this private information, arguably the best way to ensure that conversations or data transmissions stay private is by shrouding them with the dark cloak of encryption. Databases filled with private, "individually identifiable" information similarly can be protected by encryption technology in the form of controlled access schemes — i.e., requiring the use of passwords in order to enter databanks and varying levels of authorization, enforced by technological means, in order to gain access to restricted information within the database.

Technological Privacy Protection

People often have a great stake in keeping their conversations or personal data secret. In this age of staggering technological advances, however, a common perception is that it is getting harder and harder to protect one's privacy interests. Although the recent monumental increases in computing speed and memory capabilities have made the collection, manipulation, and storage of data less onerous than ever before, and have thus seemingly decreased the probability that private information will stay private, these same technological advances have also made improvements in the ways these data may be kept secure. Some of the most advanced cryptographic systems require a multitude of complicated calculations in order to turn "plaintext" (or comprehensible conversation, data) into "cyphertext" (or encrypted conversation, data). For today's computers, however, these calculations can be done in fractions of a second.

Encryption has been used for centuries to secure communications against capture by an enemy. Julius Caesar exploited a (rather simple, by today's standards) encryption algorithm to keep his military dispatches safe. The Germans used an encryption machine called "Enigma" to encode and later decode their secret messages during World War II [18]. Unbeknownst to them, however, Enigma had been "cracked" by Polish mathematicians (who later passed the information on to the French and British after Poland fell to the Germans in 1939).

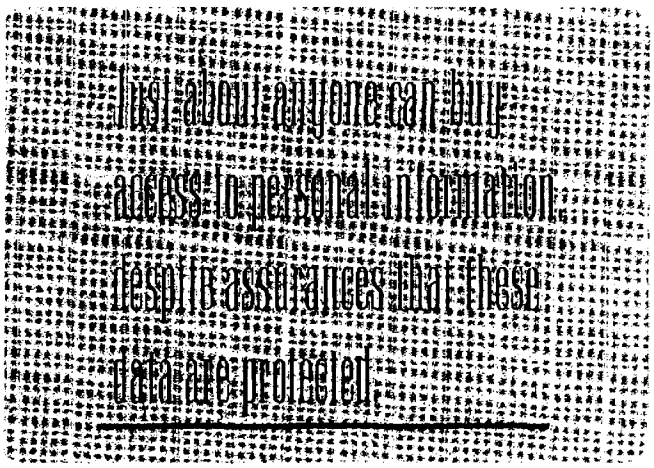
So, how does encryption work? Basically, in order to encode text, or a cellular phone communication, the words must first be converted to numbers so that later they can be mathematically manipulated. If a computer is being used to encrypt the message, the words are converted into binary numbers (bits). The simplest cryptographic system is the "Shift Cipher." In this system, the letters of the original message are simply shifted to other letters a few spaces over in the alphabet.



The problem with the shift cipher is that if Eve (a spy) were to capture the ciphertext as it makes its way from Alice (the sender) to Bob (the receiver), and if she knew that the message had been encoded using this particular cipher, she would only have to try, at the most, 25 different keys before finding the correct one to decipher the message (on average, it would take her only 26/2 = 13 tries). This encryption system is thus said to be "insecure". Even if Eve did not know what type of encryption system had been used by Alice, there are numerous tricks she could use to crack the code, based upon statistical properties of the English language (e.g., the letter "e" is the most commonly used letter, followed by "t, a, o, i, n, s, h, and r) [19]. The "substitution cipher," in which a

key is made up so that the normal, plaintext alphabet corresponds to a ciphertext alphabet of randomly placed letters (although each letter is only used once) is quite a bit more secure than the shift cipher as it has 26! (= 4.03×10^{26}) keys. The substitution cipher, however, still suffers from the same weakness to decryption via statistical methods as the shift cipher.

There are many more increasingly complicated encryption systems based upon the same general format as the shift and substitution ciphers, in which plaintext is converted to ciphertext based upon some mathematical manipulations involving a key that both the sender and receiver of the information know. In the best systems, even if Eve knows what algorithm was used to convert the plaintext into ciphertext, unless she has the key, it is impossible, or nearly so, for her to decrypt the message. One of the best of these "secret key" cryptosystems is the Data Encryption Standard (DES), developed by IBM researchers and first published in the Federal Register in 1975. DES was adopted as the standard system for encrypting "unclassified" data in 1977, and is reviewed by the National Bureau of Standards (now the National Institute of Standards and Technology (NIST)) every five years. DES uses a key with a length of 56 bits in a very complicated algorithm that encrypts plaintext in 64 bit units (bitstrings) into ciphertext that is also a bitstring of length 64. In this system, the size of the key determines how big the "keyspace" is — or, in other words, how many tries it would take to break the code if every possible key were tried successively. Thus, for a key of length 56, the keyspace is 2^{56}(= 7.2×10^{16}). Although this cryptosystem is not susceptible to cryptanalysis using statistical language methods, many think that DES's keyspace is too small for providing "reasonable" security, as a powerful computer could conceivably search the entire keyspace in about one day, thereby breaking the code. Nevertheless, DES is currently the most widely used cryptosystem worldwide [19]. Not only is it quite efficient (fast), but it may be implemented in both hardware and software products.



In the 1990s, the National Security Administration (NSA) developed an algorithm called "skipjack", that the Clinton Administration wished to make the new Federal encryption standard. This cryptosystem uses an 80 bit secret key to encrypt 64-bit input "plaintext" blocks into 64-bit output "ciphertext" blocks. Presently, the skipjack algorithm is classified, so critics are not satisfied that the code is free from "trapdoors" — or other weaknesses. In any case, according to the experts who were allowed to examine the algorithm, the skipjack cryptosystem is not vulnerable to any but "brute force", "exhaustive search" attacks [20]. As the key used in skipjack is 80 bits, as opposed to DES's 56 bits, there are 2^{24} more keys to try in the skipjack system. According to Dorothy Denning, one of the cryptography experts allowed to test skipjack, if it is assumed that the cost of processing power is halved every 1.5 years, it will take 1.5 x 24 = 36 years before the cost of breaking the skipjack code will be equivalent to breaking the DES code [21]. Of course the main concern that critics have with the skipjack algorithm is that it is part of a "key escrow" encryption system - that is, a third party keeps a copy of the secret encryption key. This concern will be addressed in a later section.

It is worth asking whether any of the fancy cryptosystems making use of very sophisticated mathematics can provide complete security. The answer is that perfect secrecy has only been proven for one system — for the others, it can only be shown that many hours of computer time would be necessary to break the code.

The one cryptosystem that provides perfect secrecy is called the "Vernam One-Time Pad." This system was developed by Gilbert Vernam in 1917 to be used in the automatic encryption and decryption of telegraph messages. The way the one-time pad works is that one chooses a key that has just as many characters (in this case bits) as the message itself and then adds the message bits to the key bits modulo 2 (in other words, the code executes an "exclusive-or" operation on the two bitstrings). Decryption is achieved by simply repeating the process (adding the key to the ciphertext (modulo 2)). Although this system is completely secure (as the key changes randomly for each letter of the message), it requires generating a key that is just as long as the message and then transmitting the key over a secure channel to the message's recipient. Furthermore, a new key must be generated for each mes-

sage sent. This cryptosystem is therefore impractical for most applications. In their chapter on encryption in *Building in Big Brother*, Deborah Russell and G.T. Gangemi, Sr. describe how keys were distributed and stored in the past as well as how they are currently managed:

> "Historically, cryptographic keys were delivered by escorted couriers carrying keys or key books in secure boxes. In some cases, this is still the way it's done. With most modern high-security cryptographic products, government agencies do the actual key distribution, delivering the keys on magnetic media to individual sites. Another approach is to distribute a master key, which is then used to generate additional session keys. A site must follow strictly enforced procedures for protecting and monitoring the use of the key, and there must be a way to change keys" [18].

Since transmitting and storing private keys is such a hassle, a more "user friendly" type of encryption system called "public key" cryptography was developed by private sector mathematicians in the mid-1970s.

In 1976, Whitfield Diffie and Martin Hellman came up with a scheme for encryption that circumvented the secret key cryptography problem of safely transmitting and storing the encrypting (and decrypting) key. What they proposed involved using a "one-way" mathematical function in order to make the encryption calculation possible using a publicly known key. Since the key that is necessary for the encryption of the message is public, there are no key transmittal concerns. In 1977, three M.I.T. professors, Rivest, Shamir, and Adleman, came up with the first implementation of public key cryptography — the RSA cryptosystem. This encryption system exploits the difficulty of finding the prime factors of extremely large numbers. Prime factoring is considered a "one-way" function, as it is extremely time-consuming to find the prime factors of a large number, whereas calculating the number once you have the factors is elementary. The way the RSA system works is as follows:

1) First, 2 large prime numbers, p and q, need to be generated. These may be obtained by using a random number generator (see, for example, ref [22]) to produce large numbers and then checking them using a Monte Carlo-type method to make sure that the numbers are prime.

2) Once p and q have been chosen, their product, $p*q = n$, and the product

$$f(n) = (p-1)*(q-1)$$

must be calculated.

3) A random number b is then chosen such that $0 < b < f(n)$ and the greatest common denominator, $GCD(b,f(n)) = 1$.

4) A second number, a, is then calculated by finding $b^{-1} \bmod f(n)$ using the Euclidean algorithm (see Stinson) [19].

5) The numbers n and b are both published — these are the public keys. The private keys, that are always kept stored safely away (i.e., in one's personal computer), are the numbers a, p, and q.

6) In order to encrypt a message, the following algorithm is used:

$$e_k(n) = x^b \bmod n$$

where $e_k(n) = y$ is the ciphertext and $x = d_k(y)$ is the plaintext. To recover the plaintext (decrypt),

$$d_k(y) = y^a \bmod n$$

is calculated.

It has been claimed that decrypting an RSA-encrypted message without knowledge of the private key is computationally infeasible [19]. It is, of course, possible to figure out the private components of the encryption key by factoring the public key component, n. Using current factoring algorithms, one can, with great difficulty, factor numbers having up to around 130 decimal digits [19]. The problem with these algorithms, however, is that the time required to do the factoring calculation increases exponentially with n ($\sim\exp(n^{1/3})$) [21].

In 1994, a 129 digit number was factored using 1600 workstations scattered all around the world. The calculation took 8 months [23]. According to Prof. H. Jeffrey Kimble, a scientist well-known in the emerging field of quantum computing, a 154 digit number can currently be factored in 4 months on 70 workstations. It would take 6 years using current technology to factor a 200 digit number. Thus, if a really secure transmission is desired, it has been recommended [19] that one choose factors (p and q) that are each at least 100 digits long when setting up an RSA cryptosystem.

One of the main problems with public key encryption schemes such as RSA is that the encryption and decryption processes involve rather complex, time-consuming, calculations. In the most efficient hardware implementations of RSA systems using a 512-bit public key, n, the rate of encryption is approximately 600 kbit/s. In a comparable DES system, on the other hand, encryption rates top 1 Gbit/s (1500 times faster than RSA) [19]. It is for this reason that Philip Zimmermann combined secret- and public-key cryptography schemes in his encryption program, "Pretty Good Privacy" (PGP).

In the early 1990s, Philip Zimmermann devised a cryptosystem

to replace DES (which he considered to be insecure) implementing aspects of both secret key and public key cryptosystems. In the PGP system, a 128 bit secret key is used to encrypt messages. This "session key" is transmitted from the sender to the recipient as ciphertext that is encrypted using the recipient's public key. Thus, time is saved by encrypting the bulk of the message using a secret key algorithm, while maintaining the convenience of public key cryptosystems.

In his PGP user's Guide, Zimmermann explains how his public key system works and in so doing, points out an important security issue of public key systems in general — authentication [24]. Whereas in most other public key systems the public keys are maintained by a central authority, in Zimmermann's system, each PGP user maintains his or her own "key ring" of public keys. Each individual using PGP, therefore, is responsible for authenticating each public key on his or her key ring. Authentication is a necessary part of public key cryptosystems simply because public keys are vulnerable to sabotage. For instance, what is to stop an impostor (say, "Eve") from posting on an Internet bulletin board, a public key that is represented to be someone else's (say, "Alice's")? If that were to happen, Eve would receive every message intended for Alice that was sent encrypted with the fake public key. Eve could then decrypt the message using her own private key, read the message, and then send the message on to Alice after first encrypting it with Alice's correct public key. No one would know (besides Eve) that the message had been intercepted.

So, how can one be sure that a public key identified as belonging to Alice, indeed belongs to her and not to an impostor? The answer lies in the process called 'authentication'. If a trusted third party has a copy of a public key that he knows is inviolate, he can vouch for it by 'signing' it using his own private key. The signed key can subsequently be checked by verifying the third party's signature using his public key (which has already been verified). Authentication may be implemented in all public key cryptosystems, and can be used not only to vouch for public keys, but to vouch for the authenticity of an encrypted message itself. In literature originally distributed by RSA laboratories, the message authentication process is described as follows:

> "Alice, to sign a message, does a computation involving both her private key and the message itself; the output is called the digital signature and is attached to the message, which is then sent. Bob, to verify the signature, does some computation involving the message, the purported signature, and Alice's public key. If the results properly hold in a simple, mathematical relation, the signature is verified as genuine; otherwise, the signature may be fraudulent or the message altered, and they are discarded" [25].

In the RSA cryptosystem, the "trusted third party," who is willing to vouch for the integrity of various public keys, is a centralized "certificate authority". One of the major companies that act in this capacity is Verisign. Before Verisign adds its signature to a client's public key, it first does a background check, verifying that the client is legitimate. Most World Wide Web browsers (e.g., Netscape and Microsoft's Internet Explorer) contain copies of Verisign's own public key, so that digital signatures generated by Verisign can themselves be verified.

The authentication process is extremely important to conducting business electronically. Not only does it protect the consumer from sending valuable credit card information to charlatans, but it protects privacy to the extent that it can prevent sensitive information from falling into the hands of unauthorized database users. Stuart A. Baker, in an article written when he was the top NSA counsel and originally published in *Wired* magazine, stresses the importance of authentication: "The real key to network security is making sure that only the right people get access to particular data. That's why a digital signature is so much more important to future network security than encryption" [26].

As a partisan allied with the NSA and the Clinton Administration, Baker promotes the view that encryption is potentially hazardous to national security and effective law enforcement. Thus, its use by private citizens should be discouraged. In an effort to encourage the use of authenticators while avoiding the murky pit of encryption, the Clinton Administration turned to NIST, which it told to select an authentication system that could be used as a Federal standard. The resulting Digital Signature Standard (DSS) incorporates the Digital Signature Algorithm (DSA). DSA is derived from the cryptosystem developed by Schnorr and El Gamal based upon the discrete log problem (another one-way mathematical function), and a Secure Hash Algorithm (SHA), which is used to reduce the message for the digital signature calculations. Most importantly (to the Clinton Administration), the DSS can be used for authentication purposes only (and not for encryption).

Critics of DSS object to the system's adoption as a federal standard for several reasons. The main difficulty with DSS, perhaps, is that its adoption as a federal standard would require a major overhaul of authentication systems already in use. Currently, the RSA

system is the most widely used authenticator [25], so converting to a new 'standard' would be burdensome. Further criticisms of DSS are that its underlying cryptosystem has not been proven secure; its signature verification process is too slow; and that the process used to select DSS as the standard was too secretive and was unduly influenced by NSA.

Encryption Policy

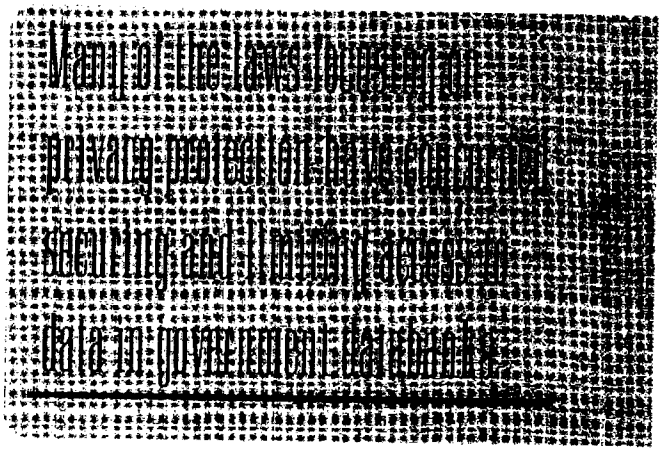
There are currently a variety of forces affecting the progress of encryption use. Pulling at one end are those people who fear that unrestricted use of encryption will endanger our nation's security — both at domestic and at international levels. On the other side are the privacy advocates, who believe that sometimes imperfect national security is a price that must be paid for individual freedom — that most important aspect of a democracy. The law enforcement side wants to write laws to limit the use of encryption. The privacy advocates want to block the passage of these laws and to develop bigger and better cryptosystems to protect privacy more effectively. Although both sides seem to understand the other side's arguments, and that any scenario must involve a compromise between privacy and freedom on the one hand, and security and public goods on the other — they each fear the balance favored by the other side.

Perhaps the most visible proponent of the law enforcement/national security agenda is Louis Freeh, the Director of the FBI. His main proposals for regulating the use of encryption have centered upon key escrow encryption systems, in which copies of secret keys are kept by a third party, and upon tight regulation of the exportation of encryption products [28], [29]. Much of the encryption legislation currently pending in Congress focuses upon both of these issues.

Exportation of Encryption

In the United States, private citizens can use both public key and secret key cryptosystems with keys of any length to encrypt their communications. Until very recently, there have been significant restrictions, however, concerning the types of encryption systems that may be exported. Currently, control of the exportation of encryption products is controlled by the Departments of Commerce and Justice. They may grant or deny exportation licenses based upon the strength of the encryption system, the uses for which the encryption systems are intended, and the destination of the encryption systems. This past January, the U.S. Department of Commerce Bureau of Export Administration (BXA) issued new encryption export regulations [52] based on recommendations from the Clinton Administration. As a result of these new rules, U.S. companies may now export encryption products around the world to non-government end-users without a license (although in most cases a prior one-time product review by BXA is still required). Furthermore, widely available "retail" encryption products may now be exported to any end-user (including foreign governments). Restrictions are still in place for exportation of encryption products to terrorist-supporting states (e.g., Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria).

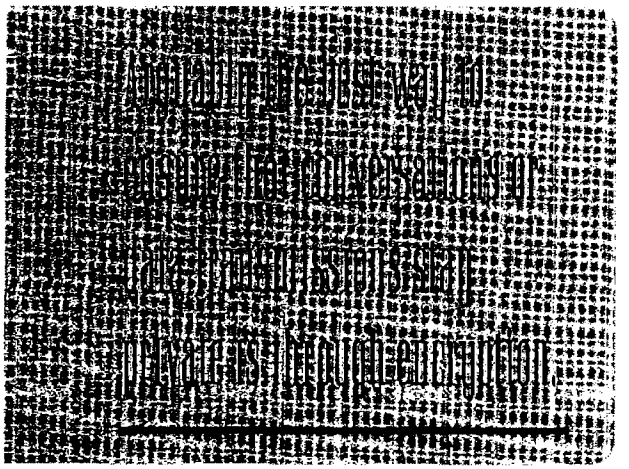
Previous to these new regulations, exportation of encryption products with keys longer than 56 bits was prohibited unless copies of the keys could be held in escrow by the U.S. government. Under the old rules, it was illegal to freely export products with DES cryptosystems, for example, despite the fact that the DES algorithm is in the public domain. Moreover, until January, even the exportation of encryption products to foreign subsidiaries of U.S. companies was restricted (these restrictions were lifted completely in January). Needless to say, the new encryption exportation regulations are cheered by industry.



Key Escrow

Key escrow encryption systems are a panacea for the law enforcement/national security community. Not only are these systems designed to provide the security of strong encryption to businesses and to individual citizens, but they are also made to accommodate law enforcement/national security interests as well. The general premise behind key escrow encryption systems is that a copy of either the private key component of a public key system or the secret key of a "regular" encryption system is held in escrow by a trusted agency. In the government's proposed system, the only people able to access the keys from the escrow agent (or agents) are law enforcement officers, who have been properly authorized to do so via a court order. The Escrowed Encryption Standard (EES) first proposed by NSA and

the Clinton Administration was implemented in the ill-fated "clipper" and "capstone" chips. Both of these chips contain the NSA's "skipjack" encryption algorithm along with various other functions related to their key escrow capabilities. Significantly, these chips are hardware, "tamperproof," manifestations of the EES, as software manifestations would not be able to protect against "reverse engineering" of the skipjack algorithm, which is classified [20]).



The clipper chip was engineered to provide encryption functions to digital communications devices. Incorporated into "secure" cellular phones, the clipper chip protects conversations between people using these phones by generating a session key for encrypting each call. In addition to the session key, a Law Enforcement Access Field (LEAF) is also produced by the chip, containing information about the identity of the chip itself as well as an encrypted copy of the session key that can be rescued via a decryption process featuring the secret keys held by the escrow agents.

The arguments that have been raised against key escrow systems are manifold. Perhaps the most cohesive and complete position paper against key escrow encryption systems is the document entitled, "The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption," written by a battalion of well-known cryptographers and computer scientists (including such luminaries as Whitfield Diffie and Ronald Rivest) [32]. According to these authors, key escrow systems contain weaknesses in three different dimensions - *risk* (i.e., compromising the proper operation of encryption systems); *complexity*; and *economic cost*.

Although there are currently several bills dealing with key escrow pending in Congress [34]-[36], most are inactive for the time being.

Future of Encryption

What will the encryption game of the future look like? It might be played out on systems that exploit the idiosyncrasies of quantum mechanics, i.e., *quantum computers*.

For example, an algorithm designed by Peter Shor, a researcher at AT&T laboratories, exploits the computational parallelism afforded by quantum computers in order to factor large numbers in polynomial, as opposed to exponential, time (see Eckert & Jozsa's paper for a good explication of Shor's algorithm [38]). Using Shor's algorithm, a 1000 digit number could be factored in only a few million steps [23], thereby collapsing the security of the popular RSA cryptosystem by making it vulnerable to computationally viable exhaustive key searches. Will the public key encryption systems based upon algorithms that are vulnerable to quantum computer attacks soon be obsolete? According to most experts, users of RSA cryptosystems have nothing to worry about on the quantum computing front in the near future. Major hurdles must be overcome before building a real-life quantum computer is possible (see [39]-[41] for discussions of possible experimental implementations of quantum computers as well as the viability of these implementations).

If quantum computing challenges the security of some popular cryptosystems, quantum *cryptography* can be seen as a ray of hope for the privacy seekers. In quantum cryptographic devices, single photon sources are used to send signals over a fiber optic cable. Since any measurement performed upon a quantum particle or system of particles disturbs, or "collapses" the system, due to Heisenberg's uncertainty principle, undetected eavesdropping on a quantum communications channel is impossible. Theoretically, then, keys for Vernam one-time pad cyrptograms could be sent securely over this quantum communications channel. Thus, completely secure messages might be sent over insecure channels using the keys that were transmitted over the quantum channel. In [42], a possible quantum communications channel is described in detail. Although there are some technological considerations that must still be addressed before a practical quantum cryptographic system can be implemented, great progress has been made in the past few years as seen in studies on teleportation [43]-[45], attack analysis [46], and coding schemes [47], [48].

Impinging on or Protecting Privacy

Technology can be used to impinge upon privacy as well as to protect it. The same can be said for legislation and all types of public rules. At the points at which they conflict, a compromise must be reached between the interests of the individual and the interests of society. How much of an individual's privacy should be relin-

quished in the interest of accommodating the public's right to security against terrorism, illegal drug trade, and all other forms of criminal malfeasance in addition to its right to access publicly-funded databanks of information? It is difficult to prescribe where the balance should be set, as there seems to be a dramatic variety of individual conceptions of privacy.

It is hard to believe that legislation restricting the use and distribution of encryption devices will accomplish its goals — hindering the malicious use of encryption by non-U.S. citizens or by domestic criminals or terrorists. Strong encryption products are already ubiquitous. Moreover, as Zimmermann bluntly puts it in his PGP user's guide, "if privacy is outlawed, only criminals will have privacy"[24]. The government simply must stay at the cutting edge of encryption and all other types of surveillance/anti-surveillance technology if it is to stay a step ahead of the criminals.

On the other hand, legislation and other rules of conduct designed to secure the privacy of personal information in databases is potentially useful. According to the authors of *Private Lives and Public Policies*, the current system in place for protecting the data in government agencies needs to be revamped [10]. Procedures for allowing restricted access to data for statistical studies need to be standardized across agencies. As the Clinton Administration seems to be content leaving the protection of privacy to market forces [49], it is unlikely that this type of legislation will be enacted any time in the near future. Technology may be able to fill this void. Some of the current work being done in the computer industry, for instance, includes research into "private information retrieval" systems — database systems designed in such a way that information from the database may be retrieved by an outside inquirer without letting the database owner learn what this information is — as well as databases set up in such a way that people can only access the information to which they are entitled, and are restricted from retrieving any other information in the database [50]. Also, it will be interesting to see if the industry pact signed by the 14 "look up services" will truly work in protecting the privacy of individuals whose personal information is contained in commercial databases. If it does not, perhaps Congress will have to resurrect one of the privacy bills that are currently "dead in the water".

In theory, there is a broad spectrum of possibilities regarding an individual's privacy. Living at either extreme — with almost complete privacy or with a virtual lack of privacy — would be painfully uncomfortable to say the least. A poignant modern example of a person who has experienced both extremes — one by choice, the other forced upon him is Theodore Kaczynski, a.k.a., the "Unabomber." Completely paranoid of technology and its concomitant evils (i.e., the role of technology in impinging upon personal freedom by facilitating the accumulation of data — and thus, power — by the government and other large bureaucracies (see "The Unabomber Manifesto" [51]), Theodore Kaczynski lived a life characterized by almost complete privacy. In order to isolate himself from the rest of society, he lived in a shack in the middle of nowhere; he interacted only infrequently, if at all, with his neighbors; in short, he had little or no contact with the outside world aside from those tenuous connections required by his anonymous acts of destruction (over which he had total control). Currently, however, Theodore Kaczynski is in jail — where he has virtually no privacy at all: All of his correspondence is monitored; all of his actions are controlled ; and many, many people know intimate details about his life and his mental health.

Luckily, most people are relatively content living in this "industrial-technological society"[48] and set the balance between their privacy and social interactions somewhere nearer the middle of the privacy spectrum than Theodore Kaczynski. The average citizen (i.e., one who does not believe that our technological society must be completely dismantled) can make some choices regarding what information he gives to whom; and by doing so, he or she can live a life that is more or less private. There are relatively easy ways to guard one's privacy: One can, for instance, simply avoid attracting the attention of government agencies or getting included in various commercial databases. Although in the United States, citizens are *required* to surrender certain bits of personal information to the government (tax information, census information), this may be construed as a price that must be paid for the privilege of citizenship. This information, however, is relatively well-protected [10]. Information that is given "voluntarily" to the government or to commercial interests, however, is not as secure. Thus, if you avoid paying for things by credit card, you will not establish a "credit history" (or, in other words, you will not accrue numerous entries in a credit agency database file in your name). If you refrain from "surfing the net," your electronic progress cannot be monitored by various "cookies," and you will not end up on numerous mailing list databases. If you forgo air travel, you circumvent the ritual x-ray invasions of privacy. There is a lot that you can do to protect your privacy, even in this Cyber Era; most of these things, however, entail giving something else up.

ACKNOWLEDGMENT

The author thanks Prof. Warren S. Warren and Prof. Burton Singer

for their helpful comments and guidance and Sheri Alpert and Wendell Davis for their evocation of interesting research topics.

REFERENCES

[1] O. H. Gandy, *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview, 1993.

[2] L. Napoli, "Federal judge halts sailor's discharge case," *The New York Times on the Web*, Jan. 26, 1998, http://www.nytimes.com.

[3] Rep. Kastenmeier, P.L. 99-508 - Electronic Communications Privacy Act of 1986;. U.S. Congress, http://thomas.loc.gov:80/home/c105query.html.

[4] D. Banisar, Big Brother Goes High-Tech, http://www.worldmedia.com/caq/articles/brother.html.

[5] N. Bernstein, "On-line, high-tech sleuths find private facts," *New York Times*, pp. A1,A20, Sept. 15, 1997.

[6] K. Lawson-Jenkins, in *Building in Big Brother*, L. J. Hoffman, Ed. New York: Springer-Verlag, 1995, pp. 76-83.

[7] A.M. Froomkin, in *Building in Big Brother*, L. J. Hoffman, Ed. New York: Springer-Verlag, 1994, pp. 413-434.

[8] F.D. Schoeman, Ed., *Philosophical Dimensions of Privacy: An Anthology*. New York, NY: Cambridge Univ. Press, 1984.

[9] S. Warren and L. Brandeis, "The right to privacy," *Harvard Law Rev.*, vol. 4, pp. 193-220, 1890.

[10] National Research Council, Social Science Research Council, *Private Lives and Public Policies: Confidentiality and Accessibility of Government Statistics*. Washington, DC: National Academy Press, 1993.

[11] Sen. Leahy, S. 376 - Encrypted Communications Privacy Act of 1997; *U.S. Senate*, http://thomas.loc.gov:80/home/c105query.html, 1997.

[12] Rep. Collins, H.R. 184 - Individual Privacy Protection Act of 1995; *U.S. House of Representatives*, gopher://unix5.nysed.gov:70/00/TelecomInfo/Reference Desk/HR 184 Privacy Protection Commission, 1995.

[13] A. Dunn, "Governments and encryption: locking you out, letting them in," *The New York Times on the Web*, Oct. 8, 1997 , http://www.nytimes.com.

[14] Rep. Markey, H.R. 1964 - Communications Privacy and Consumer Empowerment Act; *U.S. House of Representatives*, http://thomas.loc.gov:80/home/c105query.html, 1997.

[15] K. Q. Seelye, "Companies Agree to Protect Personal Data," *The New York Times on the Web*, Dec. 18, 1997, http://www.nytimes.com.

[16] J. Markoff, "Pact to test controls on data," *The New York Times on the Web*, Dec. 18, 1997, http://www.nytimes.com.

[17] Council on the Protection of Individuals With Regard to the Processing of Personal Data, European Parliament, Feb. 2, 1995. http://www.privacy.org/pi/intl_orgs/ec/final_EU_Data_Protection.html

[18] D. Russell and S.G.T. Gangemi, in *Building in Big Brother*, L. J. Hoffman, Ed. New York, NY: Springer-Verlag, 1995, pp. 10-23.

[19] Stinson, *Cryptography: Theory and Practice*. Boca Raton, FL: CRC Press, 1995.

[20] D.E. Denning, in *Building in Big Brother*, L.J. Hoffman, Ed. New York, NY: Springer-Verlag, 1994, pp. 111-118.

[21] I. L. Chuang, R. Laflamme, P. W. Shor, and W. H. Zurek, *Science*, vol. 270, p. 1633, 1995.

[22] S. Pincus and B.H. Singer, *Proc. Natl. Acad. Sci.* USA, vol. 93, p. 2083, 1996.

[23] D. Braunstein, "Quantum computation: A tutorial," Microsoft Internet Explorer, 1995.

[24] P. Zimmermann, in *Building in Big Brother*, L. J. Hoffman, Ed. New York, NY: Springer-Verlag, 1994, pp. 93-107.

[25] RSA Laboratories, in *Building in Big Brother*, L. J. Hoffman, Ed. New York, NY: Springer-Verlag, 1993, pp. 33-40.

[26] S. A. Baker, in *Building in Big Brother*, L. J. Hoffman, Ed. New York, NY: Springer-Verlag, 1994, pp. 295-301.

[27] B. Sterling, in *Building in Big Brother*, L. J. Hoffman, Ed. New York, NY: Springer-Verlag, 1994, pp. 302-306.

[28] L. J. Freeh, "FBI and Encryption - Letter to the Editor," *The New York Times on the Web*, Oct. 16, 1997, http://www.nytimes.com.

[29] P. Wayner, "FBI plan would 'deputize' private sector companies," *New York Times on the Web*, July 11, 1997, http://www.nytimes.com.

[30] J. Markoff, "A compromise on encryption exports seems to unravel," *The New York Times*, Dec. 6, 1996, pp. D1.

[31] S.T. Walker, in *Building in Big Brother*, L.J. Hoffman, Ed. New York, NY: Springer-Verlag, 1994, pp. 477-506.

[32] G. W. Turner, in *Building in Big Brother*, L. J. Hoffman, Ed. New York, NY: Springer-Verlag, 1992, pp. 460-476.

[33] H. Abelson *et al.*, "The risks of key recovery, key escrow, and trusted third-party encryption," http://www.crypto.com/key-study/report.shtml, 1997.

[34] Sen. McCain, S. 909 - Secure Public Networks Act; *U.S. Senate*, http://thomas.loc.gov:80/home/c105query.html, 1997.

[35] Sen. Burns, S. 377 - Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1997; *U.S. Senate*, http://thomas.loc.gov:80/home/c105query.html, 1997.

[36] Rep. Goodlatte, H.R. 695 - Security and Freedom Through Encryption (SAFE) Act; *U.S. House of Representatives*, http://thomas.loc.gov:80/home/c105query.html, 1997.

[37] ACLU, in *Building in Big Brother*, L. J. Hoffman, Ed. New York, NY: Springer-Verlag, 1993, pp. 409-412.

[38] A. Ekert and R. Jozsa, *Rev. Modern Physics*, vol. 68, pp. 733-753, 1996.

[39] D.P. DiVincenzo, *Science*, 270, p. 255, 1995.

[40] N.A. Gershenfeld and I.L. Chuang, Science, 275, p. 350, 1997.

[41] W.S. Warren, *Science*, vol. 277, p. 1688, 1997.

[42] C.H. Bennett, G. Brassard, and A.K. Ekert, *Scientific Amer.*, p. 50, Oct. 1992.

[43] C.H. Bennett *et al.*, *Phys. Rev. Lett.* vol. 70, p. 1895, 1993.

[44] S.L. Braunstein and H.J. Kimble, *Phys. Rev. Lett.*, 80, p. 869, 1998.

[45] A. Furusawa et al., *Science*, vol. 282, p. 706, 1998.

[46] E. Biham and T. Mor, *Phys. Rev. Lett.*, vol. 79, p. 4034, 1997.

[47] M. Koashi and N. Imoto, *Phys. Rev. Lett.*, vol. 79, p. 2383, 1997.

[48] P.D. Townsend, *Nature*, vol. 385, p. 47, 1997.

[49] J. Clausing, "U.S. official says clinton wants market-driven encryption policy," *The New York Times on the Web*, Oct. 9, 1997, http://www.nytimes.com.

[50] D.G. Marks, A. Motro, and S. Jajodia, "Enhancing the controlled disclosure of sensitive information in *Proc. Computer Security - ESORICS 96: 4th European Symposium on Research in Computer Security* (Rome, Italy) ," F. Bertino, H. Kurth, G. Martella, and E. Montolivo, Eds. New York, NY: Springer, 1996.

[51] T. Kaczynski, "The unabomber manifesto," http://www.pathfinder.com/pathfinder/features/unabomber/unifesto2.html#12.

[52] U.S. Department of Commerce, "Commerce announces streamlined encryption export regulations," press release, Jan. 12, 2000.

[53] K. Perino, "Feds release revised crypto export rules," *The Standard: Intelligence for the Internet Economy*, Jan. 12, 2000.