Payoff

Civil libertarians consider computer and communications technology to be a serious threat to individuals' personal privacy and freedom of speech. Some advocate laws to provide both an effective legal basis for accountability in the handling of personal data and procedures for redressing and compensating individuals. The development of the information superhighway may compromise personal privacy even more.

Problems Addressed

Data encryption refers to the methods used to prepare messages that cannot be understood without additional information. Government agencies, private individuals, civil libertarians, and the computer industry have all worked to develop methods of data encryption that will guarantee individual and societal rights.

The Clinton administration's proposed new standards for encryption technology—the Clipper Chip—was supposed to be the answer to the individual's concern for data security and the government's concern for law enforcement. Law-abiding citizens would have access to the encryption they need and the criminal element would be unable to use encryption to hide their illicit activity.

Cryptography and Secret Messages

Cryptography is the science of secure and secret communications. This security allows the sender to transform information into a coded message by using a secret key, a piece of information known only to the sender and the authorized receiver. The authorized receiver can decode the cipher to recover hidden information. If unauthorized individuals somehow receive the coded message, they should be unable to decode it without knowledge of the key.

The first recorded use of cryptography for correspondence was the Skytale created by the Spartans 2,500 years ago. The Skytale consisted of a staff of wood around which a strip of papyrus was tightly wrapped. The secret message was written on the parchment down the length of the staff. The parchment was then unwound and sent on its way. The disconnected letters made no sense unless the parchment was rewrapped around a staff of wood that was the same size as the first staff.

Methods of encoding and decoding messages have always been a factor in wartime strategies. The American effort that cracked Japanese ciphers during World War II played a major role in Allied strategy. At the end of the war, cryptography and issues of privacy remained largely a matter of government interest that were pursued by organizations such as the National Security Agency, which routinely monitors foreign communications.

Today, data bases contain extensive information about every individual's finances, health history, and purchasing habits. This data is routinely transferred or made accessible by telephone networks, often using an inexpensive personal computer and modem.

The government and private organizations realize—and individuals expect—certain standards to be met to maintain personal privacy. For example:

- Stored data should only be available to those individuals, organizations, and government agencies that have a need to know that information. Such information should not be available to others (e.g., the customer's employer) without the permission of the concerned individual.
When organizations make decisions based on information received from a data base, the individual who is affected by such decisions should have the right to examine the data base and correct or amend any information that is incorrect or misleading. The misuse of information can threaten an individual's employment, insurance, and credit. If the facts of a previous transaction are in dispute, individuals should be able to explain their side of the dispute.

Under strict constitutional and judicial guidelines and constraints, government agencies should have the right to collect information secretly as part of criminal investigations.

Existing Legislation

The Privacy Act of 1974

The Privacy Act of 1974 addressed some of these issues, particularly as they relate to government and financial activities. Congress adopted The Privacy Act to provide safeguards for an individual against an invasion of privacy. Under the Privacy Act, individuals decide what records kept by a federal agency or bureau are important to them. They can insist that this data be used only for the purposes for which the information was collected. Individuals have the right to see the information and to get copies of it. They may correct mistakes or add important details when necessary.

Federal agencies must keep the information organized so it is readily available. They must try to keep it accurate and up-to-date, using it only for lawful purposes. If an individual's rights are infringed upon under the Act, that person can bring suit in a federal district court for damages and a court order directing the agency to obey the law.

The Fair Credit Reporting Act of 1970

The Fair Credit Reporting Act of 1970 requires consumer reporting and credit agencies to disclose information in their files to affected consumers. Consumers have the right to challenge any information that may appear in their files. Upon written request from the consumer, the agency must investigate the completeness or accuracy of any item contained in that individual's files. The agency must then either remove the information or allow the consumer to file a brief statement setting forth the nature of the dispute.

Researchers are continuing to develop sophisticated methods to protect personal data and communications from unlawful interception. In particular, the development of Electronic Funds Transfer systems, where billions of dollars are transferred electronically, has emphasized the need to keep computerized communications accurate and confidential.

Privacy Rights

In short, the rapid advances in computer and communications technology have brought a new dimension to the individual's right to privacy. The power of today's computers, especially as it relates to record keeping, has the potential to destroy individual privacy rights.

Whereas most data is originally gathered for legitimate and appropriate reasons, “the mere existence of this vast reservoir of personal information constitutes a covert invitation to misuse.”

---

Personal liberty includes not only the freedom from physical restraint, but also the right to be left alone and to manage one's own affairs in a manner that may be most agreeable to that person, as long as the rights of others or of the public are respected. The word privacy does not even appear in the Constitution. When the Founders drafted the Bill of Rights, they realized that no document could possibly include all the rights that were granted to the American people.

After listing the specific rights in the first eight Amendments, the Founders drafted the Ninth Amendment, which declares, "The enumeration in this Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people." These retained rights are not specifically defined in the Constitution. The courts have pointed out that many rights are not specifically mentioned in the Constitution, but are derived from specific provisions. The Supreme Court held that several amendments already extended privacy rights. The Ninth Amendment then could be interpreted to encompass a right to privacy.

Federal Communications Act of 1934.
The federal laws that protect telephone and telegraphs from eavesdroppers are primarily derived from the Federal Communications Act of 1934. The Act prohibits any party involved in sending such communications from divulging or publishing anything having to do with its contents. It makes an exception and permits disclosure if the court has issued a legitimate subpoena. Any materials gathered through an illegal wiretap is inadmissible and may not be introduced as evidence in federal courts.

Data Encryption Standard
The National Bureau of Standards' Data Encryption Standard (DES), which specifies encryption procedures for computer data protection, has been a federal standard since 1977. The use of the DES algorithm was made mandatory for all financial transactions of the US government involving Electronic Funds Transfer, including those conducted by member banks of the Federal Reserve System.

The DES is a complex nonlinear ciphering algorithm that operates at high speeds when implemented in hardware. The DES algorithm converts 64 bits of plain text to 64 bits of cipher text under the action of a 56-bit keying parameter. The key is generated so that each of the 56 bits used directly by the algorithm is random. Each member of a group of authorized users of encrypted data must have the key that was used to encipher the data to use it. This technique strengthens the algorithm and makes it resistant to analysis.

Loopholes in the Traditional Methods of Data Encryption
The DES uses a 64-bit key that controls the transformation and converts information to ciphered code. There are a virtually infinite number of possible keys, so even the fastest computers would need centuries to try all possible keys.

Traditional encryption methods have an obvious loophole: their reliance on a single key to encode and decode messages. The privacy of coded messages is always a function of how carefully the decoder key is kept. When people exchange messages, however, they must find a way to exchange the key. This immediately makes the key vulnerable to interception. The problem is more complex when encryption is used on a large scale.

Diffle's Solution.
This problem was theoretically solved approximately 20 years ago, when an MIT student named Whitfield Diffie set out to plug this loophole. Diffie's solution was to give each user two separate keys, a public key and a private one. The public key could be widely distributed and the private key was known only to the user. A message encoded
with either key could be decoded with the other. If an individual sends a message scrambled with someone's public key, it can be decoded only with that person's private key.

The Clipper Controversy

In April 1993, the Clinton administration proposed a new standard for encryption technology, developed with the National Security Agency. The new standard is a plan called the Escrowed Encryption Standard. Under the standard, computer chips would use a secret algorithm called Skipjack to encrypt information. The Clipper Chip is a semiconductor device designed to be installed on all telephones, computer modems, and fax machines to encrypt voice communications.

The Clipper Chip

The Clipper Chip combines a powerful algorithm that uses an 80-bit encryption scheme and that is considered impossible to crack with today's computers within a normal lifetime. The chip also has secret government master keys built in, which would be available only to government agencies. Proper authorization, in the form of a court order, would be necessary to intercept communications.

The difference between conventional data encryption chips and the Clipper Chip is that the Clipper contains a law enforcement access field (LEAF). The LEAF is transmitted along with the user's data and contains the identity of the user's individual chip and the user's key—encrypted under the government's master key. This could stop eavesdroppers from breaking the code by finding out the user's key. Once an empowered agency knew the identity of the individual chip, it could retrieve the correct master key, use that to decode the user's key, and so decode the original scrambled information.

The Long Key.

Clipper uses a long key, which could have as many as 1,024 values. The only way to break Clipper's code would be to try every possible key. A single supercomputer would take a billion years to run through all of Clipper's possible keys.

Opponents of the Clipper-Chip plan have criticized its implementation on several counts:

- Terrorists and drug dealers would circumvent telephones if they had the Clipper Chip. Furthermore, they might use their own chip.
- Foreign customers would not buy equipment from American manufacturers if they knew that their communications could be intercepted by US government agents.
- The integrity of the “back door” system could be compromised by unscrupulous federal employees.
- The remote possibility exists that an expert cryptologist could somehow break the code.

Recommended Action

Despite opposition from the computer industry and civil libertarians, government agencies are phasing in the Clipper technology for unclassified communications. Commercial use of Clipper is still entirely voluntary, and there is no guarantee it will be adopted by any organizations other than government ones. Yet several thousand Clipper-equipped telephones are currently on order for government use. The Justice Department is evaluating
proposals that would prevent the police and FBI from listening in on conversations without a warrant.

A possible solution to these concerns about privacy invasion would be to split the decryption key into two or more parts and give single parts to trustees for separate government agencies.

In theory, this would require the cooperation of several individuals and agencies before a message could be intercepted. This solution could compromise the secrecy needed to conduct a clandestine criminal investigation, but the Justice Department is investigating its feasibility.

No method of data encryption will always protect individual privacy and society's desire to stop criminal activities. Electronic Funds Transfer systems and the information superhighway have made the need for private communications more important than ever before. Society's problems with drugs and terrorism complicate the issues, highlighting the sensitive balance among the individual's right to privacy, society's need to protect itself, and everyone's fear of Big Brother government tools.

Author Biographies

Edward H. Freeman

Edward H. Freeman is an attorney, teacher, and lecturer in West Hartford CT, with 15 years' experience in data processing, most recently with a major insurance company. He is a part-time faculty member at Central Connecticut State University.