

## **3 Encryption and Interception of Communications**

### **3.1 Overview of the Controversies**

Interception of communications (via telephone, e-mail, and the Internet) by government agencies and government attempts to restrict the use of secure encryption.

The increased use of encryption meant that law-enforcement agents could not read some communications they intercepted. Privacy advocates and civil libertarians argued for strong protection for communications using new technologies, to regain the level of privacy we had had before, while the FBI argued for increased control over telecommunications technology and restrictions on the use of encryption to regain the level of access to communications and documents it had had before.

1991: It is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law.

The phrase “plain text” in the statement means unencrypted.

The FBI’s Carnivore system sifts through millions of e-mails, looking for those of a suspect for whom the FBI has a court order.

Since 1993, the government has proposed a variety of schemes for government agents to be able to decrypt encrypted communications.

### **3.2 Intercepting Communications**

#### **3.2.1 Wiretapping**

##### **TELEPHONE**

In 1928, the Supreme Court ruled that wiretapping by law-enforcement agencies was not unconstitutional, but that it could be banned by Congress.

A 1937 Supreme Court decision ruled that wiretapping violated the law. Federal and state law-enforcement agencies and local police ignored the ruling and continued to wiretap regularly for decades, sometimes with the approval of the Attorney General.

In 1967, the Supreme Court ruled that intercepting telephone conversations without a court order violated the Fourth Amendment to the U.S. Constitution. In 1968, as part of the Omnibus Crime Control and Safe Streets Act, Congress explicitly allowed wiretapping and electronic surveillance by law-enforcement agencies, with a court order, for the first time in U.S. history.

The U.S. State Department reported that, in the late 1990s, the police and intelligence agencies of more than 90 countries routinely performed illegal monitoring of political opponents, human rights workers, and journalists.

##### **NEW TECHNOLOGIES**

E-mail and cellular phone conversations were not explicitly covered by old laws.

#### **3.2.2 Designing Communications Systems for Interception and Tracking**

In addition to sending e-mail, we shop, read news, do research, visit myriad Web sites, and send Web sites a variety of personal information. The government can learn a lot more about our habits, activities, and interests than it could from tapping telephone calls before the growth of the Web.

The FBI, arguing that new telephone technology was interfering with its ability to intercept phone calls, helped draft (and lobbied for) the Communications Assistance for Law Enforcement Act of 1994 (CALEA).

The FBI wanted requirements that all equipment be designed so that it could:

- Intercept all wire and electronic communications originating from or coming to a particular subscriber in real time, at any time (in ways not detectable by the parties to the communication)
- Perform a large number of interceptions simultaneously
- Receive intercepted communications and call-identifying information at a location specified by the government
- Receive numbers entered after the initial number dialed, with the looser justification standard that applies to pen registers
- Intercept conference calls
- Determine the physical location of cell-phone users
- Intercept packet-mode communications on the Internet.

A federal appeals court ordered the FCC to rewrite many of the rules.

### **COSTS: DOLLARS, SECURITY, COMPETITIVENESS, CIVIL LIBERTIES**

CALEA authorized \$500,000,000 for hardware and software modifications to existing telecommunications equipment to meet the demands of law enforcement.

Wiretaps were used in 90% of terrorism cases that went to trial in the 1990's. Especially after September 11, 2001, the terrorist threat is a compelling argument to many people.

There are approximately 2000 service providers. New innovations keep changing the technology. This change and diversity is frustrating to the FBI. "The prospect of trying to enforce laws without a nationwide standard for surveillance would turn enforcement into a nightmare."

#### **3.2.3 Carnivore**

Carnivore is the FBI's system for intercepting e-mail. The Carnivore system is installed at the suspect's Internet service provider (ISP). It filters all the e-mail from that ISP, examining the headers to find and copy the suspect's e-mail.

Does the FBI's sifting through millions of e-mail headers violate the wiretapping laws and the Electronic Communications Privacy Act?

In 2001, the USA PATRIOT Act allowed law-enforcement agents to use pen-register authority to get destination and time information for e-mail. (It also allowed them to get a variety of other information about people's e-mail and Internet use from ISPs, including payment information such as credit-card numbers, without a court order.)

### **3.2.4 The National Security Agency and Echelon**

#### **THE NSA**

The National Security Agency (NSA) was formed in 1952. The NSA owns and uses the most powerful computers available. Newsweek said it had nearly half the computing power in the world. The NSA monitors communications between the U.S. and other countries.

Satellite communications were a boon to the NSA; it could pick messages out of the air.

Both the physical conditions and the huge number of messages make interception of international communications in fiber optic cables extremely difficult.

#### **WHAT IS ECHELON?**

Beginning in 1998, several reports about the NSA's "Echelon" system caused a furor in Europe and the U.S.

Echelon raises issues similar to issues about Carnivore, but on an international scale.

The NSA does not need a court order to monitor foreign communications.

By intercepting messages from Iran trying to buy parts for nuclear missiles from France and phone calls of complaint from Iran to China, Echelon helped confirm that China kept an agreement to stop selling nuclear missiles to Iran.

#### **WHAT IS CONTROVERSIAL ABOUT ECHELON?**

While a system like Echelon can be of enormous benefit for learning of the plans and activities of terrorists, success is not automatic, and the many purposes to which it can be applied may distort its effectiveness.

#### **THE IMPACT OF TECHNOLOGY ON THE POLITICAL ISSUES**

How much privacy should we be expected to give up in exchange for protection from the "bad guys"?

How much information about a government's activities should be kept secret from its people in exchange for such protection?

Awareness of the technical tools used in intelligence gathering could contribute toward the development of informed answers.

### **3.3 Cryptography and Its Uses**

#### **3.3.1 Cryptography and Public Key Cryptography**

Cryptography is the making and breaking of secret codes. It is "the art and science of hiding data in plain sight." The point is to transform a message or data, called the *plaintext*, into a form that is meaningless to anyone who might intercept it.

The coded text is called *ciphertext*. The recipient of the ciphertext decodes it (this process is called decryption) and reads the plaintext message.

Encryption generally includes a coding scheme, or cryptographic algorithm, and a specific sequence of characters (e.g., digits or letters), called a *key*, used by the algorithm.

While some people are busy trying to develop good encryption algorithms, others are busy trying to develop methods to decode ciphertext. The latter endeavor is called *cryptanalysis*.

For all encryption methods used until recently, both the sender and the recipient of an encrypted message must know the key—and keep it secret from everyone else.

In the 1970s, a revolution in cryptography occurred. Whitfield Diffie and Martin Hellman developed an encryption scheme called *public key cryptography*.

Ronald Rivest, Adi Shamir, and Leonard Adleman developed RSA, a practical implementation of the Diffie and Hellman method. In this scheme, there are two mathematically related keys. One is used to encrypt a message, the other to decrypt it.

Knowing the key used to encrypt the message provides no help at all in decrypting it.

The encrypting key can be public; it is called the person's *public key*. The decrypting key is the person's *private key*.

One major advantage of public-key cryptography is that it eliminates the need to transmit a secret encryption key between the two parties.

The strength, or security, provided by an encryption scheme depends on both the cryptographic algorithm and the length of the key.

With current encryption methods and key sizes, it is extremely difficult to decode a message without the proper key, even with the government's fastest computers.

### **3.3.2 Uses of Encryption**

A few examples of private-sector applications of encryption:

- Protecting communications from unauthorized access.

Examples: e-mail, telephone.

- Protecting data in transit from unauthorized access (and manipulation for fraudulent purposes).

Examples: credit-card numbers, for purchases on the Internet; Social Security numbers or personal financial data sent to a Web site; electronic transfer of funds between financial institutions.

- Protecting stored data from unauthorized access (and alteration).

Examples: passwords and personal identification numbers stored on computer systems; bank records and other financial data (to protect against theft as well as to protect privacy); medical records; research and product-development files; personal files on home computers.

- Authentication.

Examples: digital signatures; techniques for verifying that documents have not been altered.

- Protection of intellectual property in electronic form from copyright infringement (unauthorized access and copying).

Examples: electronic books, songs, and movies sold on the Web; cable-television signals.

Football teams use radio helmets to transmit instructions to quarterbacks on the field; the transmissions are encrypted to protect them from the opposing team.

### **PROTECTION FROM THE “DOSSIER SOCIETY”**

Computer scientist David Chaum devised techniques using cryptography that make possible “digital cash” and other privacy protected transactions.

They can let us do secure financial transactions electronically without the seller acquiring a credit-card or checking-account number from the buyer.

They combine the convenience of credit-card purchases with the anonymity of cash.

These techniques provide both privacy protection for the consumer with respect to the organizations he or she interacts with and protection for organizations against forgery, bad checks, and credit-card fraud.

### **DIGITAL SIGNATURES**

For centuries, people put their signatures (or their mark) on such paper documents as contracts and checks to formalize a legal agreement or transaction.

One of the remarkable features of some public-key cryptography schemes lets us “sign” an electronic copy: The roles of the two keys can be reversed. If a message is encrypted with the private key, it can be decrypted with the public key from that key pair (and by no other key). This feature provides *digital signatures*.

The encrypted version is a signed contract because it could not have been encrypted except by using the signer’s private key.

By 2000, both the European Union and the U.S. had passed laws giving documents signed with digital signatures the same legal enforceability as those signed on paper.

There are likely to be thousands of applications of this technology.

### **CRIMINAL USE ENCRYPTION**

*Unfortunately, the same encryption technology that can help Americans protect business secrets and personal privacy can also be used by terrorists, drug dealers, and other criminals.*

-Dee Dee Myers, White House Press Secretary, 1994 (Santa Clara grad)

#### **3.3.3 Steganography**

*Steganography* is the art and science of hiding a message.

The point of steganography is to hide the fact that the message exists.

Modern steganographic methods include hiding messages within digitized documents and images.

The least significant bits of a digitized image or audio file can be changed without making a visible or audible difference; those bits can encode a message.

There are techniques to analyze digital files to detect steganographic alterations, but, if one does not know where to look, the message is safe. One research group analyzed two million files from eBay auctions in 2001 and found no hidden messages.

### **3.4 Encryption Policy: Access to Software, Keys, and Plaintext**

#### **3.4.1 Secrecy and Export Controls**

##### **SECRECY**

In an attempt to keep secure encryption methods out of the hands of enemies, terrorists, and private citizens, the government classified much information about cryptography as secret or confidential.

The NSA tried to discourage cryptography researchers from publishing their work, threatening to classify it.

##### **EXPORT RESTRICTIONS**

Throughout the 1990s, the government maintained a costly and ultimately futile policy of prohibiting export of powerful encryption software. The government implemented the policy by classifying encryption software as “munitions,” like tanks and bombs, which are subject to export control.

Phillip Zimmerman (member of the SCU Computer Engineering advisory board) developed a program using public key cryptography for e-mail. He called PGP (for Pretty Good Privacy).

In 1991, copies of PGP appeared on numerous Internet sites in the U.S. from which it could be, and was, downloaded in other countries. The government began an investigation of Zimmermann; for more than two years he was under threat of indictment for exporting encryption.

PGP was widely distributed on the Internet and became the most popular program for e-mail encryption around the world.

A survey in 1998 estimated that U.S. industry would lose 200,000 jobs and \$60 billion in the next four years because of the export controls.

By 1997, there were almost 2000 strong-encryption software packages available outside the United States.

U.S. companies tried several tactics to legally get around the export restrictions on encryption.

#### **3.4.2 Domestic Encryption Controls?**

There have never been legal restrictions on the use of encryption in the United States.

##### **KEY ESCROW AND THE CLIPPER CHIP**

In 1993, the government announced the Clipper Chip, its first attempt to ensure its access to encryption keys, and thereby created a blistering public controversy.

The Clipper Chip and several of the government’s later proposals used a form of *key escrow*. That means that a copy of the encryption keys is kept by some organization other than the user of the encryption. The organization is called an *escrow agent*. Law-enforcement agents, with a court order, could get a key from an escrow agent.

The government dropped its goal of widespread use of the Clipper Chip because of technical flaws and political opposition.

## **KEY RECOVERY**

There are good business and personal reasons for using some sort of key-recovery system. If a company employee is not available and someone else in the company must read files that were encrypted by the employee, there is a problem.

When commercial key escrow and key recovery develop as services available in the market, there are no major political issues.

## **VOLUNTARY OR COMPULSORY?**

One of the big weaknesses of key-escrow and key-recovery schemes was that, even if they were widely adopted, drug dealers and terrorists could use other devices and software to encrypt their messages.

## **THE NATIONAL RESEARCH COUNCIL REPORT**

In the midst of the encryption controversies, Congress requested that the national Research Council (NRC), the research affiliate of the National Academy of Sciences, do a through study of U.S. encryption policy and make recommendations.

It argued that strong encryption provides increased protection against hackers, thieves, and terrorists who threaten our economic, electric-power, and transportation infrastructures. It argued that the free market and business needs for data protection would do a better job than the National Security Agency and the FBI. It said that plans that rely on government escrow of keys would have security and liability risks,

## **IS THE GENIE OUT OF THE BOTTLE?**

Cypherpunks and others who support our right to use whatever technical means to choose to protect our privacy are fond of saying, “The genie is out of the bottle.”

Strong encryption is so widely available that governments cannot stop its use.

Increases in computer power make older encryption schemes almost worthless. In the same year that Adi Shamir described a system to crack RSA encryption with 512-bit keys, he also cracked the code used in millions of cell phones worldwide.

### **3.5 Fundamental Issues**

#### **3.5.1 The Role of Secrecy**

To maintain its control over cryptography and access to communications, the government has regularly used secrecy—of cryptographic research, its wiretapping difficulties caused by new technology (in the CALEA debate), its algorithms (in the Clipper Chip), its software (Carnivore), and everything about Echelon.

There are, however, problems with secrecy.

More than one expert has suggested that the security of our vast communications and financial systems, and the economic health of our technology export business, may be more important to our national security than being able to read secret messages of potential enemies.

#### **3.5.2 The Ever-Changing Status Quo**

In defending its efforts to obtain the plaintext of communications, from Clipper Chip to key escrow to CALEA to Carnivore, the FBI argued repeatedly that it was not asking for any new

powers; it was just maintaining the status quo. To the FBI, the status quo was the fact that they could intercept and read any communication they wanted.

The “unbreakable” 512-bit RSA of the 1990s is now threatened, and longer keys are used. A new technique under development, called quantum computing, could threaten the secure codes of today. A new technique, called quantum cryptography, might lead to new unbreakable codes. There is no good reason why the status of privacy or the government’s ability to intercept and decode communications at a particular time should be adopted as a moral or political standard just because it is the status quo.

### **3.5.3 Trust in Government**

We have seen abuses of wiretapping by the FBI and local police agencies throughout the 20<sup>th</sup> century. We have seen abuses by the NSA. We have seen that the government was not completely honest in its early claims that it did not intend to impose any restrictions on the encryption American citizens could use.

Zimmermann said Americans do not understand why he is so paranoid about the government, “but people in police states, you don’t have to explain it to them. They already get it, and they don’t understand why we don’t.”

How much should the freedom and privacy of honest and peaceful people be weakened to aid the government’s law-enforcement activities? How far can we trust the government not to abuse its power?

To some people it seems so obvious that legitimate law-enforcement needs require that the government have access to any communication (with a court order). To others the potential for abuse is the overriding concern.

### **HOW MUCH DOES TECHNOLOGY MATTER?**

*In western countries, with the development of ingenious electronic devices, Big Ears and Big Eyes hide in the deep blue sky. Satellites see us in action in our backyard, and if needed, our conversations are wiretapped by some powerful agencies...In less developed countries, surveillance is realized by human eyes and ears. In Vietnam where the freedom of speech is “legally” banned, I remember being taught to listen to family members and report conversations having some specific keywords, such as “communism,” “United States,” “old government” ...and I would have done it for the good of my country. I’d witnessed kid-heroes sending their families to concentration camps. Without freedom of speech, with fear of speaking, we listened with resignation.*

-Thuc Luu