FROM
"THE END OF PRIVACY"
BY C. SYKES

10

■

Breaking the Code:

The Fight over Encryption

First a layman's primer on encryption. The technology itself may be mind-foggingly complex, but its applications and significance are relatively easy to understand. Despite its techie-trappings, cryptography is the essence of privacy in the electronic world.

Essentially, encryption enables anyone to send an electronic communication that can be read by only the person to whom it is sent. It provides security for everything from voice communications and e-mail to the electronic transfer of funds. Without encryption—or encoding—electronic communications such as e-mail are comparable to sending a postcard; such communications are open and easily read by third or fourth parties. Encryption is the envelope, the seal that keeps the communication private. It is also the reasonable guarantor of security for everything from health records to fund transfers to love letters.

Historian David Kahn traces the private use of encryption back four millennia to the ancient Egyptians. The Hebrew scribes of the Old Testament's Jeremiah also used a cipher, and Julius Caesar pioneered the use of codes for military purposes. "It must be that as soon as a culture has reached a certain level," Kahn has written, "probably measured largely by its literacy, cryptography appears spontaneously—as its parents, language and writing, probably also did. The multiple human needs and desires that demand privacy among two or more people in the midst of social life must inevitably lead to cryptology wherever men thrive and wherever they write."[1]

Encryption can also be a powerful tool to conceal plots and nefarious deeds. But as Carl Ellison notes, the same can be said of any arrangement

that allows individuals to be sheltered from public scrutiny. "It is true that cryptology can give privacy to individuals trying to meet electronically (by videoconferencing, conference calls, etc.)," he writes, "but individuals have always had both an opportunity and a right to privacy. Sometimes this is achieved by meeting in a closed room or an open field. Sometimes it is achieved through cryptology. Citizens used this privacy to make love, to confess to a priest, to confer with a lawyer, to meet in various Anonymous twelve-step groups, to hold business meetings, to plan new inventions or product releases, to plan sales strategies, to have a pleasant chat with friends, and to engage in innumerable other innocent pastimes. In addition to this, some individuals use privacy to plan criminal activities.

"It would help law enforcement greatly," Ellison notes, "if every conversation in the last category were relayed directly to the appropriate agency to be tape recorded and used both to guide investigations and to be presented as evidence in an eventual court trial. However, there is no way to achieve this selective privacy."[2]

The most adamant advocates of encryption are the so-called cypherpunks, such as Eric Hughes. The author of the "Cypherpunk's Manifesto," Hughes has little faith in voluntary self-regulation, or the restraint of government.[3] His analysis is electronic-age realpolitik. "We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. It is to their advantage to speak of us, and we should expect they will speak." But he also rejects European-style legislation or regulations that seek to protect on-line privacy because such regulations defy the fundamental and immutable laws of information in an information society.

"Information does not just want to be free, it longs to be free . . . ," declares Hughes, *"information is fleeter of foot, has more eyes, knows more, and understands less than Rumor."*

What this means is that if we are to expect any privacy we can count neither on the goodwill of our neighbors, the restraints of the powerful, nor the power of law. We are on our own; it is up to individuals to find creative ways of communicating and dealing with one another in ways that allow for anonymity.* But the very technology that erodes privacy also

*Hughes distinguishes privacy from secrecy. "A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want any-

provides the possibility of a strong privacy unknown to previous generations. "People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do." The bulwarks of the new strong privacy, Hughes declares, are cryptography, anonymous mail-forwarding systems, digital signature, and electronic money.

LOCK AND KEY

Until quite recently, encrypting electronic communications on a routine basis was not practical. Under old encryption technology both the sender and the receivers needed to have the same secret key—one to encode the communication, one to unlock it and read it. The problem with this is that it is both cumbersome and vulnerable to attack. But the modern history of encryption began in 1976, when Whitfield Diffie and Martin E. Hellman developed an alternate—and much easier—approach to encryption. Instead of two secret keys they proposed using a "public key" and a "private key." The public key, as its name suggests, is freely available and can be accessed by anyone who wants either to use or copy it. This is what you would use to send a communication. When the intended recipient gets your message, though, he must use his own private key—which no one else knows—to unlock the code. Another way to understand how this works, suggests Bruce Schneier, is to think of the two codes as a lock and key. "The world doesn't need a new lock design for every front door. It is enough to have one lock design, and hundreds of thousands of different

---

body to know. Privacy is the power to selectively reveal oneself to the world." For Hughes, the key to privacy in the electronic age is making sure that each party to a transaction has the knowledge only "of that which is directly necessary for that transaction." That requires we reveal as little as possible. "When I purchase a magazine at a store and hand cash to the clerk, there is no need to know who I am."

The key to assuring privacy in an open society, is the availability of "anonymous transaction systems"—a notable example of which is cash. In an electronic age, cryptography and its related technologies would serve the save function.

"Privacy in an open society also requires cryptography. If I say something, I want it heard only by those for whom I intend it. If the content of my speech is available, I have no privacy. To encrypt is to indicate the desire for privacy, and to encrypt with weak cryptography is to indicate not too much desire for privacy. . . ."

keys."[4] The advantage of the public and private keys is that there is no special handling required, no transmissions of code words, or numbers. The same technology can be used to verify the identity of both senders and recipients, by creating a digital signature.

The keys are codes generated by computers; they can be numbers, strings of numbers, words—it does not really matter. What does matter is the length of the key. Simply: The longer the key, the more bits, the harder it would be to crack the code and thus the safer the communication. In the world of cryptography, *bits matter.* A code that uses a 56-bit key, for example, could probably be cracked in a matter of hours; one that used an 80-bit key would take 10^7 years, a 112-bit key would take 10^{17} years and a 128-bit key would take 10^{22} years to crack.[5]

ENTER THE SPOOKS

The resurgence of academic interest in encryption in the mid–1970s was paralleled by increasingly aggressive efforts by the nation's intelligence establishment to slow and/or control the new technology. Not surprisingly, the agency most intimately involved in the issue was the National Security Agency, which undoubtedly boasts the most sophisticated code-breaking technologies and the most advanced information-gathering apparatus in the world.

NSA richly deserves its hyper-spooky reputation. Even the most intrusive technologies for invading privacy pale in comparison to the NSA's surveillance systems, such as Echelon, which is operated in conjunction with intelligence agencies in Great Britain, New Zealand, and Australia. Even for a century that has grown used to being watched and listened to, the implications are disconcerting. "Within Europe," a report to the European Parliament declared, "all e-mail, telephone and fax communications are routinely intercepted by the United States National Security Agency, transferring all target information from the European mainland via the strategic hub of London, then by satellite to Fort Meade in Maryland via the crucial hub at Menwith Hill in the North York Moors of the UK."[6]

Such watching and listening is clearly a major priority for intelligence agencies. According to a report by the conservative Free Congress Foundation, the Echelon site at Menwith Hill in Great Britain is the largest spy station in the world, with a staff of 1,400 NSA personnel and 350 staffers

from the UK Ministry of Defense.*[7] The report to the European Parliament described Echelon as a worldwide surveillance apparatus that "stretches around the world to form a targeting system on all of the key Intelsat satellites used to convey most of the world's satellite phone calls, Internet traffic, e-mail, faxes and telexes." The system works by positioning ships, satellites and intercept stations across the globe—in New Zealand, Hong Kong, the United States, Australia, and Great Britain—which have the capability of capturing nearly every satellite, microwave, cellular, and fiber-optic communication on the planet. Wrote analyst Patrick Poole: "Having divided the world up among the UKUSA parties, each agency directs their electronic 'vacuum-cleaner' equipment towards the heavens and the ground to search for the most minute communications signal that traverses the system's immense path."[8]

What makes Echelon especially noteworthy is that unlike many of the other electronic spy systems developed during the Cold War, Echelon is designed "for primarily non-military targets: governments, organizations and businesses in virtually every country." The report to the European Parliament described Echelon as operating by "indiscriminately intercepting very large quantities of communications" and then analyzing all of the data using extraordinarily sophisticated artificial intelligence technology which listens, reads, and sifts the communications for key words, phrases, names, or places to "tag." Once tagged, the intercepted communications are captured, transcribed, and then forwarded to the intelligence agencies of the countries that might find them of interest. Each of the five countries in the system gets to contribute to the so-called "dictionaries" used by Echelon to identify special words and phrases in the intercepts. But the truly Orwellian power of the Echelon system is its capacity to filter, decrypt, and analyze the messages it captures. Echelon reportedly uses futuristic com-

*Writes Patrick Poole: "The backbone of the ECHELON network is the massive listening and reception stations directed at the Intelsat and Inmarsat satellites that are responsible for the vast majority of phone and fax communications traffic within and between countries and continents. The twenty Intelsat satellites follow a geostationary orbit locked onto a particular point on the Equator. These satellites carry primarily civilian traffic, but they do additionally carry diplomatic and governmental communications that are of particular interests to the UKUSA parties."

puters systems like the Silkworth system at Menwith Hill, which employs voice recognition, optical-character recognition and data-information engines to sift the messages. Other systems can "flag" an individual's voice pattern, so that the surveillance system can capture every conversation that person makes.

How might such powers be abused? We do not need especially active imaginations to imagine the possibilities. There have already been suggestions—some from whistle-blowers—that Echelon's technology was used to intercept real-time telephone conversations involving a United States senator and possibly a congressman.[9] In late 1998, the NSA was forced to acknowledge that Diana, Princess of Wales, whose file ran to 1,056 pages, was among those caught in its surveillance web. Though Diana was not a specific target, NSA's eavesdropping dragnet was so comprehensive that it picked up hundreds of *mentions* of the princess, apparently right up until the moment of her death.[10] The *London Observer* has reported that Echelon's data net has also snagged communications involving such groups as Amnesty International, Greenpeace, and a missions organization known as Christian Aid. But the possibilities for using such intercepts to win a business advantage may be even more tempting than political snooping. As the stakes of world trade grow, the edge provided by insider information about strategies, prices, and terms is increasingly invaluable.

In 1995, the *New York Times* reported that both the NSA and the CIA station in Tokyo had provided crucial detailed information to the U.S. trade representative whose negotiators were locked in difficult talks with Japanese car companies. A Japanese newspaper subsequently charged that the NSA was monitoring confidential communications among Japanese companies.[11] In 1994, intelligence agencies intercepted phone conversations between a French company and Brazilian officials who were in the market for radar systems.[12] The reports from the intercepts were forwarded to the American competitor, Raytheon Corporation. Other reports have linked NSA intercepts to negotiations over satellite deals involving Indonesia and oil and hydroelectric deals in Vietnam.[13]

As if that were not enough, European Union states, the parliament report said, have also signed a memorandum of understanding in 1995 agreeing to set up an international phone-tapping system that would include forcing network and service providers to install easily "tappable" systems.

THE NSA CAMPAIGN

Despite these extraordinary powers, the NSA was deeply worried that the spread of powerful encryption technology might interfere with its ability to watch and listen. At the urging of the security agencies, the U.S. government has treated encryption technology the same as it treats dangerous munitions, and has jealously restricted its export—even though it is easily available from vendors around the world. In the early 1970s, the government tried to control the market for encryption by setting the national standard—known as the Data Encryption Standard, or DES—at a mere fifty-six bits. One does not need to be a computer scientist to realize that the standard was set at a level that the NSA would have little trouble decoding. Indeed, in 1998, a group of cryptographers cracked the DES in less than three days using a machine they built for less than $250,000, proving that the government's standard could be decoded both quickly and cheaply.[4]

Under Director Bobby Ray Inman, the NSA also tried to put a damper on the development and dissemination of cryptographic know-how to the public by targeting academic research. At one point, an NSA operative went so far as to suggest that the NSA had exclusive control over the funding of research into encryption, but he later backed off. In an attempt to classify even those encryption products designed by nongovernment research, the NSA next tried to limit the ability of American scientists to present papers at scientific conferences, citing the 1951 Invention Secrecy Act. When two of their first targets, Professor George Davida of the University of Wisconsin and freelance researcher Carl Nicolai, received an order from the NSA declaring their work classified and ordered them not to discuss it in public, the two researchers not only refused the order but went public with the NSA's heavy-handed threat. Faced with publicity and brewing academic backlash, the agency backed off and rescinded its order, which it claimed was a mistake.[15]

Inman's next gambit was to declare encryption a threat to national security and call for limits on the public dissemination of encryption. "There is a very real and critical danger that unrestrained public discussion of cryptographic matters will seriously damage the ability of the government to conduct signals intelligence," he insisted.[16] The scientific community was outraged. "If you want to win the Indianapolis 500, you build the fastest car; you don't throw nails on the track," gibed the president of As-

sociation for Computing Machinery. Undeterred by the criticism, Inman asked the American Council on Education in 1983 to conduct a study on the limits on academic research on the subject. The ACE panel rejected the idea of restrictions on the dissemination of technical information on encryption, but endorsed the voluntary submission of papers to the NSA. So repugnant was the notion, however, that no scholars outside the agency itself permitted the NSA to vet their work.[17]

Throughout the 1980s the NSA pushed hard not only to keep the encryption genie in the bottle, but also to have a hand in the developing telecommunications superstructure.* Its clout would become apparent in the fight over the Clipper Chip.

THE CLIPPER CHIP

One of the early drafts of the wiretap bill would have explicitly banned the use of any encryption not authorized by the government. But in 1991, the Justice Department, NSA, and CIA had to agree that a flat ban on encryption would prove too controversial. So it was dropped for the time being.[18] But it was never off the table.

*In 1984, the Reagan administration gave the agency broad authority over computer security by designating the NSA—rather than the National Bureau of Standards—as the national manager for Telecommunications and Automated Information Systems Security. A second directive in 1986 gave the NSA even wider powers, which it seized with considerable vigor and enthusiasm. During the mid-1980s, the NSA used its new authority to send agents to visit private companies, including Lexis/Nexis, DIALOG, CompuServe, as well as financial institutions. Mead Data Central, the parent company of Lexis/Nexis reported one visit by five government agents, representing CIA, the NSA, and the FBI.

In part because it had overstepped its boundaries, in 1987 Congress passed the Computer Security Act, reaffirming the National Bureau of Standards as the point-agency for protecting the security and privacy of nonclassified information. Although the legislation was designed to reaffirm civilian control, the NSA continued to play a central role in the issue, both undermining and co-opting its rival agencies.

†In a memo to Defense Secretary Dick Cheney, the director of the CIA and the attorney general, Brent Scowcroft, President Bush's National Security Advisor, noted that "Success with digital telephony [the wiretap bill] will lock in one major objective; we will have a beachhead we can exploit for the encryption fix; and the encryption access options can be developed more thoroughly in the meanwhile."

Unfortunately for the intelligence agencies, both the technology and the marketplace threatened to outrun the NSA's ability to control the process. In September 1992, AT&T announced that it would begin to market a telephone encryption device called Surity 3600, which would sell for $1,100. The FBI and other agencies were both surprised and alarmed and, for a time, considered threatening AT&T with legal action if the company did not drop the idea of marketing a scramble-phone. But AT&T's move also provided the government with an alternative.

If the spooks could not ban nongovernmental encryption outright, the next-best option was to control the market for encryption technology. To do that, they would have to force the marketplace to accept the NSA's own encryption devices, which would enable private citizens and businesses to keep their communications private and secure from everyone . . . except the government. The technology the agency had in mind was known as Skipjack, but it was code-named "Clipper."[19]

The NSA "Clipper" would scramble any communications, *but the government would hold the key to them all.* After intense discussions between AT&T and the Justice Department, the telecommunications company agreed to drop its own device and instead adopt the Clipper for its new phone. In return, the company hoped, the government would make the NSA technology the new national standard.

That is exactly what President Clinton did. The final decision to go ahead with the Clipper Chip was made at a March 31, 1993 meeting attended by the vice president and the attorney general as well as the NSA, the CIA, and the Office of Management and Budget. A little more than two weeks later, the president announced his support for the Clipper as the new national standard, which was quickly followed by an order from the Justice Department for 9,000 new Clipper phones from AT&T. Under the guidelines issued by the Justice Department, the keys to the Clipper would be held by two government agencies with ties to the intelligence agencies and law enforcement. In theory, the agencies would release the "escrowed" keys only when they received the proper order, but under the Justice Department's rules they would be exempt from any sanctions for violations of the procedures. Individuals whose communications were intercepted would have had no rights to object or even to suppress the data.[20]

If Clinton thought that the market-based gambit would be accepted, he was quickly undeceived. Reaction was immediate and overwhelming. A Time/CNN poll found 80 percent of the public opposed the idea of the Clipper proposal.[21] The *Christian Science Monitor* editorialized: "The government should not be in the business of asking manufacturers to build secret backdoors into their equipment, particularly when government holds the keys."[22] And *Business Week* asked: "Will the Information Superhighway enable the federal government to become a high-tech snoop on a scale undreamt of in George Orwell's worst nightmares?"[23] Perhaps the most devastating critique came from columnist William Safire, who described the Clipper as a proposal that "we turn over to Washington a duplicate set of keys to our homes, formerly our castles, where not even the king in olden times could go."

"The clipper chip . . . would encode, for Federal perusal whenever a judge rubber-stamped a warrant, everything we say on a phone, everything we write on a computer, every order we give to the shopping network or bank or 800 or 900 number, every electronic note we leave our spouses or dictate to our personal digit-assistant genies.

"Add to that stack of intimate data the medical information derived from the national 'health security card' Mr. Clinton proposes we all carry. Combine it with the travel, shopping and credit data available from all our plastic cards, along with psychological and student scores. Throw in the confidential tax returns, sealed divorce proceedings, welfare records, field investigations for job applications, raw files and CIA dossiers available to the Feds, and you have the individual citizen standing naked to the nosy bureaucrat."[24]

Ignoring the scope and vehemence of the public opposition, the Clinton administration nevertheless announced on February 4, 1994 that it was formally adopting Clipper as a "voluntary" government standard. The "voluntary" part was largely for political cover because the Justice Department and the NSA continued to push manufacturers hard to adopt the Clipper standard, hoping to create a large enough market to make Clipper the de facto national standard—relegating other forms of encryption to the fate of the Betamax. At the same time, NSA began a campaign to convince other countries to adopt the Clipper standard themselves. Understandably, however, many of the foreign governments were more than a little reluctant to use a chip in all of their communications whose key was held by the NSA.

The effort was a nearly complete bust. Many of the AT&T devices bought by the federal government in the first flush of enthusiasm for the Clipper reportedly gather dust in government warehouses.[25]

THE HAPPY-FACE CLIPPER

The failure of Clipper did not mark the end of the government's attempt to limit private encryption. Beating a tactical retreat, the administration decided that nongovernmental encryption would be permitted . . . as long as the keys to every code were handed over to a "trusted third party" instead of a government agency. However, both the software and "third parties" would have to be certified by law-enforcement and intelligence agencies if the software was to be exported. Shortly after Vice President Gore outlined his support for "key escrow," privacy advocate Marc Rotenberg labeled the new policy "Clipper with a happy face."[26]

Apparently assuming that it would never occur to lawbreakers to find ways of avoiding insecure communications, the FBI began pushing legislation to make key-escrow systems mandatory—in other words, making it illegal for Americans to encode their communications without handing over the keys to a government-approved agency. And the administration's briefing papers bluntly declared that government lawyers had concluded after studying the issue that "Americans have no Constitutional right to choose their own method of encryption."[27]

In practical terms, the proposed laws would mean that every computer or system that used a security code would have to give a copy of that code to a government-approved third party. That would affect every set of medical records, as well as every cash machine, vending system, and on-line communications system. The idea of "key escrow" was an example of technological wishful thinking and legal chutzpah. Technically, it assumed that a system could be designed so that (1) it would provide security and safety for the "keys" handed over to third parties without creating nightmarish new system weaknesses, and (2) there was a practical way of also assuring that the government could get "covert access, ubiquitous adoption, and rapid access to plain text." Experts questioned both assumptions. "Keyholders" would have to manage literally billions of codes, which would be changing daily. Holding them accountable for failures or lapses would either be extremely difficult or simply impossible.

The proposal also marked a novel approach to the relationship between

citizens and their government. For two centuries, the Fourth Amendment had protected citizens against unlawful searches and seizures. But now the administration was not only demanding that citizens, in effect, hand over keys to their front doors and personal files, but it would also make them criminals if they refused to comply. Storing or keeping any information in a way that the government could not easily read would now be a federal crime.*[28]

The administration's policy received another rude setback in mid–1996, when a panel of the National Research Council issued a 450–page report which not only endorsed the wide use of privacy-enhancing encryption, but warned against the passage of any new laws restricting encryption. The report by the NRC's Committee to Study National Cryptography Policy even suggested that it was the government's own antiencryption policies that might pose the greatest threat, because weak encryption not only made business, but also the nation itself more vulnerable to mischief. "If cryptography can protect the trade secrets and proprietary information of businesses and thereby reduces economic espionage (which it can), it also supports in a most important manner the job of law enforcement. If cryp-

*Gore's new policy also continued to sharply restrict the expert of encryption technology, limiting any codes to a mere sixty-four-bits. As Rotenberg noted, the administration was "trying to force America's software companies to include government-sought key-escrow features in its software as the price for export approval." Under the federal regulations, the government continued to treat encryption as munitions technology—treating it the same way it would a machine gun—and therefore subject to severe export restrictions. The logic of the ban apparently was that U.S. companies would be reluctant to create two different brands of software—one for domestic sale, another for export—and that they would therefore market only weak encryption systems. But the fact was that encryption was easily available throughout the world. There were numerous free encryption programs, including PGP—which stands for Pretty Good Privacy—which was offered free over the Internet. In 1993, an international study found more than 350 different encryption products from foreign companies in twenty-two different countries. By June 1996, Trusted Information Systems found that the number of encryption products had risen to 532 products from twenty-eight countries. Commenting on the futility of the government's efforts, Bob Kohn, general counsel for PGP, quipped: "The export law is like building a chain-link fence in the middle of the ocean to keep the water out." (Ashley Dunn, "Governments and Encryption: Locking You Out, Letting Them In," *New York Times*, October 8, 1997.)

tography can help protect nationally critical information systems and networks against unauthorized penetration (which it can), it also supports the national security of the United States."[29]

Underlining the extraordinary and exceptional nature of the government's attempt to regulate encryption, a survey found that the United States was virtually alone among free, industrialized countries in attempting to control the right of its citizens to keep their digital communications and information private. Countries that had followed the FBI's lead and imposed domestic controls on encryption included China, Pakistan, Russia, Singapore, Israel, and Belarus. Although France also had a quite restrictive policy, the government there announced plans to ease its controls to "allow French companies to fully enter the marketplace of electronic commerce currently dominated by U.S. companies." Other than that, almost every democratic, industrialized country in the world permitted their citizens to use, manufacture, and sell encryption technology without any legal limits.[30] In late 1997, the European Commission explicitly rejected proposals to restrict cryptography or set up key-escrow systems. Taking a radically different tack than American law-enforcement agencies, the EC report argued that "restricting the use of encryption would well prevent law-abiding companies and citizens from protecting themselves against criminal attacks. It would not, however, permit criminals from using these technologies."[31]

But the FBI continued to push hard for limits. During a congressional hearing, FBI Director Louis Freeh declared: "[W]e're in favor of strong encryption, robust encryption. The country needs it, industry needs it. We just want to make sure we have a trapdoor and key under some judge's authority where we can get there if somebody is planning a crime." Moreover, the political dynamic seemed to favor the FBI. "When it comes right down to it," reporter Brock Meeks wrote, "your privacy rights don't stand a snowball's chance in hell of outweighing pictures of dead babies or pieces of dead babies." And Freeh was not at all shy about invoking images of rampant terrorism that might be unleashed in an encrypted world. "The FBI," Freeh insisted, "cannot and should not tolerate any individuals or groups . . . which would kill innocent Americans, which would kill America's kids."[32]

The bombing at the 1996 Olympics and the crash of a TWA flight to

Paris (which was, for a time, believed to be the work of terrorists) gave extra momentum to sweeping counterterriorism measures that would have dramatically increased the government's surveillance capabilities.*[33]

Freeh clearly viewed the spread of encryption with alarm. "The drug cartels are buying sophisticated communications equipment . . ." he warned Congress. "This, as much as any issue, jeopardizes the public safety and national security of this country. Drug cartels, terrorists, and kidnappers will use telephones and other communications media with impunity knowing that their conversations are immune from our most valued investigative technique."[34] Not only was the administration seeking tougher controls on encryption, it also sought authority to allow multipoint—also known as "roving"—wiretaps—a shift that would allow the government to wiretap *individuals* as well as locations.

The political appeal of the FBI's warning became apparent in the congressional debate over legislation regulating computer privacy. Civil libertarians, the computer industry, and privacy advocate had rallied around a bill proposed by Congressmen Zoe Lofgren of California and Bob Goodlatte of Virginia, known as the "Safety and Freedom through Encryption Act" (SAFE) that would have outlawed key escrow and would have eased the government's control on the export of the technology. Initially, the bill seemed headed for easy passage; it was cosponsored by more than 250 members of the House and was easily approved by the House Judiciary and International Relations Committees. But when Congress returned from its August 1997 recess, supporters faced a full frontal assault from the FBI and the Clinton administration. FBI director Freeh pushed hard for his own proposal to manage key escrow and toughen the export controls and, in mid-September, he won a stunning victory against the forces of computer privacy.

In the space of a week, the house National Security Committee voted to actually toughen export controls on encryption and the House Select

*The Clinton administration specifically announced: "We will seek legislation to strengthen our ability to prevent terrorists from coming into possession of the technology to encrypt their communications and data so that they are beyond the reach of law enforcement. We oppose legislation that would eliminate current export barriers and encouraging the proliferation of encryption which blocks appropriate access to protect public safety and the national security."

Committee on Intelligence passed legislation that appeared to create government controls over virtually every kind of software in existence. Not only did the committees endorse legislation requiring every computer user to supply the government with a set of spare keys, it also outlawed the use of *any* program that could not be easily accessed and read by government agents. The legislation was so sweeping that critics warned that it would "effectively outlaw software as we know it." Ratcheting up the pressure on Congress, Freeh had urged the tougher legislation in a series of "classified briefings" behind closed doors. That secret testimony, which emphasized the threat from criminals and terrorists, persuaded House members to opt for the most extreme antiprivacy proposals on the table.[35]

Taken literally, the Freeh plan would have banned the use of any code system that his agency could not easily break. As Peter Wayner noted in the *New York Times*, "The latest approach is to ban virtually everything and presumably let the prosecutors decide what qualifies as encryption." He noted that one early version of the proposed ban on codes was so sweeping that it "would seem to include all computers, paper, chalkboards, cereal-box decoder rings, writing instruments, and the arms of baseball managers telling their players what to do."[36] After these setbacks, privacy advocates quickly recovered and the House Commerce Committee rejected the FBI plan on September 24, 1997.[37] Six months later, the FBI announced that—at least temporarily—it would no longer push for the encryption controls.[38] The agency's retreat came only weeks after the *New York Times* reported that the battle over encryption was threatening President Clinton's political support in Silicon Valley.[39] Rather than reflecting a change of heart on the part of the FBI and the NSA, the decision to back off (for the time being) seemed to be a response to political arm-twisting from the White House.

Despite continued jockeying over the issue of export controls, however, the issue was never definitively laid to rest, and the victory for privacy advocates rested on the shakiest possible political ground. A single terrorist incident would quickly revive the proposals, especially if the episodes occurred at a time when the political parties are vying with one another for the mantle of toughness on crime. Savvy privacy advocates also recognized that the defeat of the more radical antiprivacy measures pushed by the FBI had the effect of making other attempts to regulate encryption seem more moderate in comparison. One proposal—known as McCain-Kerrey—would not overtly mandate the use of key escrow, but would

effectively have forced it as a national standard. Under the legislation, any network either created by the federal government or financed in any way by the government would be compelled to hand over its "key" to a government-approved third party.[40] On top of that, the government would be allowed to purchase only those encryption products that allowed easy access to the keys. What could not be accomplished de jure would be accomplished de facto.[41]

The history of the government's attempts to provide itself with a trapdoor into the nation's communications system explains the intensity of the reaction to the Intel Corporation's decision to install a "unique identifier" in its new Pentium III chips and to the revelation that the Secret Service had been quietly bankrolling a private company that was buying up tens of millions of driver's-license photos to create a national database. In both cases, the government appeared to accomplish indirectly what it could not achieve directly.

As in the case of the Clipper Chip, law enforcement's best hope may now be for private technology companies to embrace new (government-approved) standards providing for easy government access to communication. Given the political realities, it is unlikely that the FBI could ever have persuaded Congress to give it the right to plant tracking devices into every personal computer. But no law prevents the Intel Corporation—or any other company that dominates the marketplace—from doing so, thus providing the government precisely the access to personal communications that it was unable to get through the front door. The only flaw in such a plan is its assumption that consumers will accept such standards. It also assumes that competitors will not exploit the decision of companies like Intel which choose to sacrifice their customers' privacy.