FROM
"THE LIMITS OF PRIVACY"
BY A. ETZIONI

3

DECIPHERING ENCRYPTED MESSAGES

A PROLONGED DEADLOCK AND AN UNHOLY WAR

AMID VERY JUSTIFIED PUBLIC CONCERNS about the loss of privacy, surprisingly little attention has been paid to the creation of what might be called "hyper-privacy." It is based on encryption (basically a very complicated code that protects the secrecy of the communications involved), the advanced forms of which are very difficult, some believe impossible, to crack. The introduction of these very powerful codes, or hyper-encryption, dramatically alters the balance between privacy and the common good—in favor of the former.

The explosive increase in electronic communications and commerce since the inception of the Internet has led to a large and growing market for encryption technologies. Businesses use encryption to protect themselves against espionage by competitors and foreign governments and to establish secure links with their partners, suppliers, and customers. Banks and investment houses rely on it to ensure the confidentiality of their transactions. Charles Schwab, for instance, re-

ported that, as of 1998, half of all its business was done on the Internet.[1] Individuals draw on it to protect their private communications and confidential documents.

Encryption is spreading quickly. As of September 1997, Trusted Information Systems of Glenwood, Maryland, had identified 1,601 encryption products manufactured and distributed by 941 companies in at least 68 countries. Of these, 59 percent were produced in the United States, and 41 percent were produced in 29 other countries.[2] Encryption software is also freely available on the Internet.

As it becomes easier and more automatic to use, encryption is being integrated into commercial applications and network protocols. Word processing, spreadsheet, database, electronic mail, Web browsing, Internet telephony, and other software applications will soon incorporate encryption systems that use codes that are 128 bits or longer. Dorothy Denning and William Baugh Jr., two leading experts, believe that these cannot be cracked. As they put it, "At 128 bits, finding an encryption key by exhaustively checking all possibilities is not even feasible in a lifetime using all the computers in the world."[3]

To appreciate the importance of these developments, one must note the increase over the last few years not only in the volume but also in the proportion of communications of all sorts—commercial and political, personal and public—that is conducted in cyberspace. A much smaller proportion of the total volume of communications is now relayed through old-fashioned technologies such as "snail mail" and phone calls, and that proportion is shrinking fast.[4]

Although hyper-encryption greatly enhances privacy in the cyberworld, it poses new and rather difficult barriers to public authorities as terrorists, drug lords, pedophiles, and other criminals increasingly draw on the new forms of encryption. As of the end of 1998, there was no agreement, either within the public or in Congress, on whether new laws should be enacted that would allow the U.S. government to acquire a special new capability to decipher encrypted messages.

As encryption has improved by making codes ever stronger, public authorities have found that they cannot break the codes on their own. The Washington scuttlebutt is that the National Security Agency (NSA) has spent $5 billion trying to break the strongest codes and failed to do so. The government has repeatedly stated that public

safety requires that it be granted, by the parties involved, the "keys" needed to decipher their encrypted messages; the business community and cyber-libertarians, however, object strenuously. The White House, under the leadership of Vice President Al Gore and Ira Magaziner, has negotiated with these parties—to no avail.

Should public authorities have the capability to decipher encrypted messages? Will public safety be seriously hampered if public authorities are unable to do so? What is the main source of danger to the public—the eavesdropping state (Big Brother) or the "Criminal Element"[5] that uses hyper-encryption? Can privacy (which encryption helps protect) and the common good (including national security and domestic peace) be reconciled, at least in part, by limiting the conditions and situations in which encrypted messages may be deciphered by public authorities?

Even if a policy acceptable to all concerned is suddenly found, or the whole matter becomes obsolete as a result of new technological developments,[6] there is still much to be learned from the study of the government's argument that it must be able to decipher strong encryption as a matter of public safety, and of the opponents' objections in defense of privacy and other individual rights.

In the following discussion, I consider first the argument of those who see a need for public authorities to be able to decrypt coded messages, drawing heavily on the work of the Georgetown University computer science professor Dorothy Denning and her associate William E. Baugh Jr.[7] I then examine the concerns raised by civil libertarians and cyber-libertarians, especially by Professor A. Michael Froomkin of the University of Miami School of Law and Professor Ron Rivest of MIT, who fear that public decryption would grossly violate individual rights, particularly privacy, and is impractical, unnecessary, or both.

THE THREAT TO LAW ENFORCEMENT AND NATIONAL SECURITY

As a result of the increasing use of strong encryption, law enforcement officers are no longer able to crack numerous privately encrypted communications and transactions. Encryption has already provided

criminals and terrorists with a powerful tool to conceal their activities. Aldrich Ames, a CIA official who spied on the United States for the Soviet Union, encrypted files on his personal computer. Members of the Aum Shinri Kyo (Supreme Truth) cult, which launched a deadly nerve gas attack on the Tokyo subway in 1995, encrypted computer files that contained details about their plans to inflict mass destruction in the United States.[8] Ramszi Yousef, who was a member of the international terrorist group responsible for bombing the World Trade Center and a Manila Air airliner, encrypted files on his laptop computer pertaining to additional plans to blow up eleven U.S.-owned commercial airliners in the Far East.[9] After the bombing of the U.S. embassies in Kenya and Tanzania in 1998 it was revealed that the CIA had foiled three other attacks in 1997 by using electronic interceptions.[10] These would not have been possible if the terrorists had used strong encryption.

Denning and Baugh report an especially illuminating case:

> Dutch organized crime has an information warfare division that combines muscles, brains, know-how, guts, and money to achieve their goals. Dutch organized crime uses encryption in their attempts to evade law enforcement. They get technical support from a group of skilled hackers who themselves use PGP (Pretty Good Privacy) and PGPfone to encrypt their communications. The hackers at one time supplied the mobsters with palmtop computers on which they installed Secure Device, a Dutch software product for encrypting data with the International Data Encryption Algorithm (IDEA), which uses 128-bit keys. The palmtops served as an unmarked police/intelligence vehicles database. In 1995, the Amsterdam Police captured a PC in possession of one organized crime member. The PC contained an encrypted partition, which they were unable to recover at the time.[11]

SPECIFIC THREATS OF ENCRYPTION

Denning and Baugh detail five threats posed by encryption to law enforcement, public safety, and national security.

1. Encryption can make it impossible to obtain necessary evidence. For instance, they report, one investigation of intellectual property theft was put on hold because the evidence, believed to be contained in en-

crypted files, was inaccessible. In another case, the inability to decrypt a hard disk blocked an investigation. It is true that sometimes the suspects may be convicted anyway, but generally not of the crimes believed to be concealed by encryption. For example, a pedophile suspected of serious corporate espionage pled no contest to multiple counts of distribution of "harmful materials" to a juvenile. The evidence that authorities thought might support charges of corporate espionage could not be decrypted. FBI Director Louis Freeh testified before Congress in 1997 that his agency was unable to assist with five requests for decryption in communications intercepted in 1995, and twelve in 1996.

2. Encryption can frustrate communications intercepts that reveal valuable information about the intentions, plans, and membership of criminal organizations and generate leads for criminal investigations. Drug cartels rely heavily on communications networks; monitoring of these networks has played an important role in identifying the leaders and illegal proceeds of these cartels. Such surveillance is becoming more difficult as these organizations rely increasingly on strong encryption programs, which the Cali cartel of Colombia already reportedly uses in its telephone communications.

Encryption is also employed to conceal information regarding the victims of crimes. For instance, in pedophilia cases, the inability to decrypt can make it impossible to identify victims in need of psychological counseling. Encryption poses problems even when it is used by the victims of crime. Senator Charles Grassley told a hearing in June 1997 about an eleven-year-old boy who committed suicide after being sexually molested. At the time of his testimony, the police were unable to decrypt the boy's personal organizer, which investigators thought might contain information about the man the boy's mother believed had molested him. The investigation had been on hold for over a year.

3. Encryption can frustrate antiterrorism efforts. Denning and Baugh report that electronic surveillance has been used to thwart a significant number of terrorist acts, including assassinations, the bombing of a foreign consulate, a rocket attack against a U.S. ally, the shooting down of a commercial airliner with a stolen military weapons system, an attack on a nuclear power facility, and a rocket attack against an FBI field office. If the communications in these cases had been en-

crypted, the planned catastrophes might not have been averted. Even if the codes had been cracked, doing so might have taken too long for the results to be useful, especially if the keys changed with each message or phone call.

4. Encryption can hinder the gathering of intelligence. Communications intercepts conducted as part of foreign intelligence operations provide information that is valuable for national security, including intelligence about military operations, hostile political powers—particularly those with weapons of mass destruction—and weapons proliferation and terrorism. All these intercepts would be significantly hindered by encryption.

5. Encryption, oddly enough, may lead to greater violations of privacy than would otherwise have occurred. For example, if investigators encounter unbreakable encryption on a wiretap, they may well pursue other methods of surveillance, including hidden microphones, cameras, and other sensors installed on the subject's premises. Undercover operations are another alternative. These methods—which are quite legal under certain conditions—are often not only more dangerous to the subject and to law enforcement officials, but also more invasive of the subject's privacy.

A SIGNIFICANT AND MACROSCOPIC DANGER?

As I suggested earlier, the first criterion for a policy evaluation is determining whether there is a significant macroscopic problem. In the case at hand, the question of whether public safety will be significantly endangered if public authorities are unable to decipher encrypted messages is answered with an unqualified affirmative by leading experts such as Denning and Baugh. Additional documentation to this effect has been presented to the Congress by FBI Director Freeh and Deputy Attorney General Jamie Gorelick.[12] Given that the most ominous dangers that decryption purports to avert are still hypothetical, one may ask whether they justify the determination that we face a significant and macroscopic problem. In the Introduction, I mentioned the constant warnings that we face this or that hypothetical catastrophe—from the year 2000 bug to flesh-eating bacteria—most of which turn out not to justify diminishing privacy to further the common

good. If we look closely at the dangers that decryption is supposed to fight, we find that no one so far has carried out the scenario often cited as a major rationale for enabling public authorities to breach encryption: No one has actually held a city for ransom, threatening that unless fellow terrorists are released a nuclear bomb will be detonated or a biological or chemical toxin released.[13]

Consideration should be given, however, not only to the probability that a given event will occur but also to the magnitude of the disaster if it does. Events that have a very low probability but a very high disutility (such as the terrorist scenario depicted) deserve as much public attention as those that have a rather high probability but a *relatively* low disutility (e.g., the acts of individual drug leaders or pedophiles). In short, even if nuclear, biological, and chemical terrorism seem unlikely, the tremendous magnitude of such threats justifies taking specific measures to protect the public. The fact that there is significant danger to the public, however, does not justify taking any and all measures to protect it. Strong encryption may pose a serious problem for those concerned with public safety and national security, but the ways of coping with the problem must be considered carefully, especially if some diminution of privacy and other rights is involved.

VOLUNTARY PUBLIC KEY RECOVERY: A SECOND-CRITERION TREATMENT

Given that relying on voluntary action (a second-criterion treatment) is preferable to coercive measures (third-criterion intervention), the question arises: Can we protect national security and ensure public safety in this area by relying only on voluntary actions?

It might seem on the face of it that voluntary approaches to problems associated with national security, public safety, and traffic in controlled substances hardly make sense. But as a matter of fact, the main approach advocated by the U.S. government in the case of encryption has been from the very beginning a largely voluntary one.

Voluntary public key recovery aims to help users protect their information while making criminal investigations less difficult. A *key recovery* system is a backup system for encryption keys. The objective is to ensure that encrypted data are decipherable even if the primary copies

of the keys are inaccessible or destroyed, either accidentally or intentionally. The backup facilities can be managed by the individuals and organizations that use encryption (self-recovery) or by an independent firm (third-party recovery). The adoption of *public* key recovery, which entails depositing a key with public authorities or in places they can access, is of great potential benefit to law enforcement.

Law enforcement seeks public key recovery for two purposes: decrypting stored files and e-mail messages in cases involving court-ordered searches and seizures of computing resources, and decrypting communications—in real time and without the knowledge of the parties involved—in cases that involve court-ordered wiretaps.[14] A private organization may prefer to operate its own key recovery service so as to retain control over its keys, but law enforcement, for obvious reasons, generally prefers third-party key recovery agents and agents who are within their jurisdiction. If organized crime groups operate their own key recovery facilities, criminals might very well fail or refuse to cooperate with the authorities. Moreover, as with wiretaps, decryption must be performed surreptitiously to have value. Investigators cannot approach the targets of their investigations to ask them for the recovery keys.

Initially the United States offered users of encryption a choice: They could freely use whatever encryption software they could find on the market (or the Internet), or they could purchase a more powerful program (powered by the Clipper chip's Skipjack coding algorithm) provided by the U.S. government. The latter would include a key allowing U.S. law enforcement authorities to decipher the messages.[15]

Critics argue that such a voluntary approach is futile because people can purchase strong encryption programs from other countries.[16] For instance, Representative Bob Goodlatte (R-Va.) wrote in response to a *Washington Post* editorial supporting export controls:

> The editorial fails to mention that strong encryption products are already available from foreign manufacturers and on the Internet. German, Dutch, Swedish, Russian, Irish and other foreign producers are creating strong and reliable encryption products, and reputable U.S.

firms are willing to stake their corporate reputations on the quality of those products.[17]

The government still has a point. Those who gain encryption from sources other than the U.S. government cannot rely on programs downloaded from the Internet, which may be unreliable or include trapdoors that can be exploited by unknown parties. Also, although an American can purchase strong encryption programs in several other countries, many countries also insist on embedding access keys.[18] Thus, individuals or corporations purchasing a Russian or French program would have to worry about public authorities in those countries deciphering their messages.[19] Still other countries may declare that they do not include a backdoor in their encryption programs but have few qualms about including one anyway. If the United States encouraged other countries to join a treaty that allows public authorities access to encrypted communications when called for, a rogue state, some critics argue, might not agree to participate. This possibility, however, has not stopped countries from formulating bans on land mines, the hunting of whales, the use of polychlorinated biphenyls (PCBs), and much else. The fact that such an initiative by the United States is not exactly what the industry and the cyber-libertarians are calling for reveals that their opposition is based on grounds other than the impracticality of public decryption when other countries are involved.

Finally, critics maintain that government-sponsored voluntary public key recovery is unlikely to last: As stronger and stronger encryption is used by private parties, the government will be pushed to ban the use of uncrackable encryption unless it is provided with keys, thereby terminating the voluntary approach.

The critics seem to have been correct about this last point. As of 1998, powerful encryption programs are available on the market from what seem to be trustworthy sources.[20] Moreover, the U.S. government seems to be moving toward seeking legislation that would *require* providers of encryption to include key recovery in their packages and make it accessible, if necessary, to public authorities.[21] Although the policy of relying on voluntary participation has not changed, the FBI began in 1997 to advocate legislation that would require key re-

covery in domestic encryption products. A 21 July 1997 letter to Congress from the presidents of the International Association of Chiefs of Police, the National Association of Attorneys General, the National Sheriffs' Association, and the National District Attorneys' Association supported the FBI's position: "We are in unanimous agreement that Congress must adopt encryption legislation that requires the development, manufacture, distribution and sale of only key recovery products and we are opposed to the bills that do not do so."[22] It should be noted, however, that both the second- and third-criterion approaches are unacceptable to most critics. Their arguments, many of which concern the protection of individual rights, deserve close examination.

THE BASES OF THE OPPOSITION

The main opposition to public decryption, both voluntary and mandatory, has come from a coalition of select profit-making businesses (especially makers of computers and software), which seek to remove limits on their right to export their products, and various individualists,[23] including civil libertarians and cyber-libertarians. Some of the more outspoken members of this informal coalition are engaged in what has been repeatedly referred to as a "holy war" against the government.[24] The coalition has marshaled enough public opposition to decryption by public authorities that Congress has balked at enacting the needed legislation. Moreover, the Clinton administration has found it impolitic to exercise its administrative power to order the Department of Justice to proceed.

One major line of criticism concerns the limitations the U.S. government has put on the *export* of strong encryption programs. Although these limitations have gradually been lifted, allowing for the export of ever stronger programs, critics have continued to argue that the controls simply mean loss of business and jobs for Americans because other countries can produce strong encryption programs without a key recovery element.

Representative Goodlatte has observed that "our export restrictions do not keep strong encryption out of the wrong hands. They serve only to keep American industry from fully competing in the global marketplace." Goodlatte adds, as supportive evidence, a statement by former British Prime Minister Margaret Thatcher: "Governments are

. . . themselves 'blind forces' blundering in the dark, obstructing the operations of markets rather than improving them."[25]

It is difficult to establish whether these foreign or privately produced American encryption programs are as strong as the one the American government originally offered to provide, and whether they are free of hidden trapdoors. Because my main concern is not with commercial issues but with the balance between privacy and the common good, I do not explore here the question of whether profits and jobs should take precedence over other considerations in the marketing of encryption software in other countries.[26] Rather, the key question is whether the government is justified, given that stronger and stronger encryption systems are available on the open market, in requiring private users to enable public authorities to decrypt their messages. If the answer is yes, under what conditions should such access be granted?

PRACTICAL OBJECTIONS

In this case as in others, individualists raise both practical and principled objections to measures recommended to enhance public safety. Some critics maintain that criminals would not use encryption systems that public authorities could "read," that criminals would simply purchase software overseas so that they would not have to fear such eavesdropping. Thus, public key recovery would burden or ensnarl only law-abiding citizens. William Safire put it well, if with tongue in cheek:

> Ah, but wouldn't it be helpful to society to have instant access to the encoded communications of a Mafia cap, or a terrorist ordering the blow-up of a skyscraper, or a banker financing a dictator's nuclear development? Sure it would. That's why no self-respecting overlord or terrorist or local drug-runner would buy or use clipper-chipped American telecommunications equipment. They would buy non-American hardware with unmonitored Japanese or German or Indian encryption chips and laugh all the way to the plutonium factory.[27]

Despite these protestations, there are many reasons to believe that key recovery might nevertheless help law enforcement cope with criminals.

1. As I mentioned earlier, several countries already demand that systems built in their country include key recovery capabilities by public authorities.[28] In other words, criminals may find it a bit more difficult to find trustworthy, reliable programs than Safire and others assume.
2. Those who download the encryption software freely available on the Internet usually cannot determine who may have built trapdoors into it—competitors, other nations, hackers, or perhaps even Interpol.
3. Social scientists, like myself, who put tape recorders in plain view of people they interview (only after having obtained their explicit permission, of course) often find that people quickly forget about these recorders and say things they may not necessarily like to have recorded. Criminals who use phones often overlook the possibility that they may be tapped. Indeed, Webster Hubbell forgot that all phone conversations from prison are recorded and made several comments he surely would have preferred not to share with authorities and the world. President Nixon, of course, got into quite a bit of trouble because he forgot that he was being recorded. In the same vein, there are good reasons to assume that if encryption is built into most means of communication, criminals will often continue to act as they do now.
4. The pressure on criminals *not* to use most communication systems, if they feared decryption on all but their own specialized equipment, would help law enforcement.
5. Given that there is no reason for most law-abiding people to use systems that contain no public recovery features, the deliberate use of other systems would point public authorities toward those communication systems in which sophisticated criminals were concentrated. This point is conceded by critics.

There are those who are concerned that such knowledge would give the government too much power. For instance, Philip Zimmermann, a cyber-libertarian, makes an analogy to the use of postcards: "Anyone who use[s] an envelope would draw suspicion because while everyone is using a postcard [he] decided to use an envelope, therefore he must

have something to hide."[29] Actually, we face this situation daily, and very few object to such obvious uses of information by public authorities. Thus, if the Drug Enforcement Administration (DEA) knows that drug dealers frequent certain airports more than others, it puts more of its agents and sniffing dogs in those locations. Similarly, the police are out in greater force at night than during the day and concentrate their efforts in high-crime areas. So far nobody has demanded that public authorities ignore such information and distribute their efforts randomly. There seems no reason to treat cyberspace differently.

Whenever I have asked individualists whether they would support a key recovery system, or some other way for public authorities to crack encryption, if their technical and practical objections could be overcome, they have retreated to principled objections. One cannot but conclude that even though the practical objections are the first line of attack (and the one with the most universal appeal, because if a system cannot be made to work, few will favor it, whatever their political or ideological position), the most profound individualistic objections rest on principle.

PRINCIPLED OBJECTIONS: COME A TYRANT . . .

Cyber-libertarians argue that even if one could trust the current government with key recovery, a tyrant might someday come along and abuse the system. Says Zimmermann:

> Sometimes in a democracy bad people can be elected, and if democracy is allowed to function normally, these people can be taken out of power by the next election. But if a future government inherits a technology infrastructure that's optimized for surveillance, where they can watch the movements of their political opposition, they can see every bit of travel they could do, every financial transaction, every communication, every bit of e-mail, every phone call, everything could be filtered and scanned and automatically recognized by voice recognition technology and transcribed. . . .[30]

Rivest has written:

> The Clipper proposal places all trust for its management within the executive branch; a corrupt president could direct that it be used for inappropriate purposes. The unspecified nature of many of the associated procedures leaves much room to speculate that there are "holes" that could be exploited by government officials to abuse the rights of American citizens. Even if the proposal were modified to split the trust among various branches of government, one might still reasonably worry about possible abuse. Merely because you've met the current set of representatives of various agencies, and feel you can trust them, doesn't mean that such trust can be warranted in their successors.[31]

If the American government were ever to be captured by a tyrant, Americans would have much more to worry about—and fight against—than the abuse of public decryption keys. There is no reason to deny that the existence of such keys, even if carefully escrowed, could help some future Stasi. But hobbling the ability of public authorities in a democracy to protect people from drug dealers and other criminals is much more likely to create social conditions under which strong-armed leaders will be invited to restore law and order. Historically, tyrannies have arisen not because liberties were gradually eroded, but because breakdowns in social order were not effectively dealt with by hobbled democracies. Such is the lesson of a recent American experience, if on a much smaller and local scale. When the elected government of the District of Columbia was replaced by an appointed board in 1995, citizens complained very little, because the elected government had failed to provide for public safety or respond to many of the citizens' most elementary needs. Similarly, New York City embraced Mayor Rudolph Giuliani in 1993, and readily reelected him four years later, despite his high-handed methods, because crime was running out of control and the city was considered ungovernable.

American public authorities currently face a new barrier to investigatory work as a result of the spread of strong encryption programs. To deny them the tools they need to determine what happens beyond this barrier, under all circumstances, is to unsettle the delicate balance between safety and privacy—to the neglect of the common good.

MORE PRINCIPLED OBJECTIONS: VIOLATIONS OF THE CONSTITUTION?

Individualists often assert that the suggested measures to enhance public safety in this area violate Americans' right to privacy, chill free speech, undermine liberty, endanger the freedom of association, and are otherwise highly intrusive. Because some of these assertions are so general and sweeping in scope, they provide no specifics one could examine and thus should be treated as expressions of concern rather than as fully developed arguments. There are, however, some carefully laid out arguments that can be closely evaluated. Many of these have been made by Michael Froomkin, a highly regarded and frequently cited legal scholar who has written two important articles on the subject.[32]

Froomkin assesses the effects of a prohibition on the use of strong cryptography (i.e., with no key recovery features) in terms of privacy rights and First, Fourth, and Fifth Amendment rights. I will briefly summarize and respond to these arguments without examining Froomkin's numerous subpoints and asides.

Froomkin argues that privacy, the right to be let alone, is violated when individuals are required to disclose information about themselves, something that he claims occurs when public key recovery is introduced.[33] He argues that such keys also violate another privacy right, "the right to autonomous choices regarding intimate matters," because people exchanging escrowed messages in intimate matters would no longer be able to do so in reliable privacy.

Froomkin further maintains that law enforcement key recovery violates the First Amendment because by disclosing matters people prefer to keep secret, the possibility of recovery compels speech. Such keys also chill speech because people may fear that others might be listening in. Additionally, he believes these keys diminish freedom of association because some people are willing to band together only under conditions of anonymity.

Froomkin also suggests that the very existence of law enforcement key recovery constitutes a warrantless search—a violation of the Fourth Amendment. And he believes that the Fifth Amendment re-

stricts the introduction of key recovery by public authorities because decryption entails self-incrimination.[34]

The ACLU has embraced a similar position, although Froomkin focuses on mandatory systems while the ACLU strongly opposes voluntary systems as well.[35] The rights organization's reasons are laid out in a page on its Web site:

> Free speech: In one recent case, a computer scholar wrote a new encryption program but when he submitted it for export approval, he was told that not only was his code a "munition," but even a paper he wrote about it could not be sent abroad. A federal court disagreed, ruling that encryption is a form of speech protected by the First Amendment.
>
> Compelled speech: If encryption is speech, then being required to give your key code to the government is a form of forced, or compelled speech—also prohibited by the First Amendment.
>
> Academic freedom: Classifying encryption technology as a form of munitions compromises academic freedom, since academics must refrain from discussing their work with foreigners (considered exportation), and American instructors are afraid to teach encryption technology to foreign students—even in their stateside classrooms.
>
> Search and seizure: The Fourth Amendment protects people from unreasonable searches and seizures. A blanket requirement that all individuals, whether or not they are suspected of criminal activities, turn over their encryption keys to the government, or its licensed agents, is an unconstitutional seizure. The government should foster privacy protection through encryption technology—not demand the keys to our telephone, computer and online privacy.[36]

On 23 September 1997 a group of law professors wrote an open letter to the House Commerce Committee, opposing key recovery.[37] The letter is particularly important because it conveys the opinions, not of extremists, but of thirty legal scholars, including some at well-known law schools such as Harvard, UCLA, and Stanford. *The letter*

addresses only the professors' concern that various rights might be violated; it does not even mention, let alone seek to address, any public safety concerns.

The letter opens with the statement: "We write to express alarm about an unprecedented proposal that has been advanced to impose criminal penalties on the manufacturing or distribution of domestic encryption products that do not contain a government mandated 'backdoor.'" The proposal was "in large part drafted by the FBI"—apparently prima facie evidence against the proposal. The professors argue: "Never in peacetime has our government attempted so completely to monopolize a single form of communication; never has it required, in effect, a license to exercise the right to speak." The analysis of the alleged violations of rights mirrors closely the arguments made by Froomkin, one of the signatories.

THE DIFFERENCE BETWEEN LAW-ABIDING CITIZENS AND "CRIMINAL SUSPECTS"

The various objections raised by the ACLU, Froomkin, and other constitutional scholars—their concerns that privacy and First, Fourth, and Fifth Amendment rights, among others, will be violated by public key recovery—all assume that the government could and would use at will this power to listen in arbitrarily on the conversations and search the documents of "all individuals," "Americans," or "all free people."[38]

Interceptions of this sort would indeed be the equivalent of the government arbitrarily listening in on telephone conversations, opening mail at will, or placing microphones in people's homes. One can readily concede that such wanton and large-scale intrusions on privacy might well cause the assorted unconstitutional and antidemocratic effects that individualists fear. However, the arrangement the government proposes, and which various individualist groups and their business allies continue to reject and effectively block, is not at all addressed by these critics. To demonstrate this point, it is necessary to reexamine precisely what the government wants to be able to do, as well as the constitutional principle this capability is based on.

The government seeks the capability to decipher messages, but this capability would be activated only after independent judicial approval.

The government would have to make a specific case that there was sufficient reason to suspect that criminal activities had taken place, and that evidence was likely to be found in encrypted communications. Once a judge was convinced of the validity of these claims, he or she would authorize the issuance of a warrant to decipher a specific set or flow of communications. In short, decryption would be governed by the same procedural safeguards as wiretaps. (There are some exceptional conditions—for instance, a national emergency—under which warrants are not required and other judicial procedures are used for the tapping of telephones. These exceptions might apply to decryption as well, but because they are just that—very exceptional—they are not discussed here.)

In addition, although the government initially suggested that it should be responsible for holding the keys (split between two agencies, to minimize further the possibilities of unauthorized use), it has since offered a compromise to allay fears of abuse by the government: The keys would be deposited with third parties (trustees or even private corporations).

Let us assume that the government has specific and credible evidence that someone is holding a kidnap victim, but the FBI is not sure where. Evidence to this effect is presented to a court, which then grants (as other courts have under similar circumstances) the government the right to tap the suspected kidnapper's phone. The suspect, fearing such tapping, pushes a button on his phone and thus encrypts some of his calls. It seems illogical to allow tapping and "reading" of the calls if they are transmitted in one form, but not to allow the use of the technical measures needed to "read" the same calls transmitted on the same lines but in some other form. In other words, despite some technical differences, *key recovery is basically an updated tap.* To argue that the government is permitted to tap regular phone calls, even if the callers are using some kind of coded language (many criminals use code words or dialects they believe few know), but not to eavesdrop on encrypted messages, is no more logical than to suggest that the government may search and seize old-fashioned paper files (if granted a warrant) but not computerized ones.

One may argue that phone taps are legally introduced only *after* court approval, but that the *capacity* to decrypt messages must be in

place *before* such action. This, however, is a distinction without a difference. The capacity cannot be legally *activated* without a court order. Indeed, the proposed law enforcement key recovery provides additional protection in the form of third parties or trustees and split keys, safeguards that phone taps do not have.

To put it differently, our system of justice assumes that there are three kinds of people: most citizens, whose rights are fully intact; criminals who have been convicted and thus have many of their rights suspended while they are incarcerated; and those "criminal suspects" who are *legally* suspected of having committed a crime and whose status is thus in between ordinary citizen and convicted criminal—some of their rights have been suspended, but not as many as those of convicted criminals. (I stress "legally" because it is not sufficient for a police officer to claim someone is a suspect and then treat him or her as such; as already indicated, evidence must be presented, and so forth, before anyone becomes a criminal suspect.) For instance, under certain conditions the government can restrict people's movements (for instance, by asking them to surrender their passports) and detain them for short periods of time even though they have not yet been indicted, let alone convicted, of any crime.

Even the ACLU, although it is always seeking to raise the bar that determines whether reasonable suspicion has been legally demonstrated, accepts that if the government has made its case, its claims have been subject to sufficient scrutiny, and a warrant has been issued—effectively transforming an ordinary citizen into a legal suspect—public authorities may search such a suspect's home, read his mail, and tap his phone. Under key recovery, it is these kinds of individuals, not "all individuals," and not "all Americans," who would have his messages decrypted by public authorities. To imply that the mere existence of a capacity for law enforcement key recovery turns all Americans into suspects is like arguing that because phone lines run outside homes, and hence are accessible to public authorities without the active knowledge of those who are tapped, the privacy and freedom of all Americans is violated.

Because much rides on the question of whether key recovery constitutes a greater violation of privacy than phone taps, I compare next the steps involved in each process.

When public authorities have specific and credible evidence that a person has committed a crime, they present that information to a court, and if the court finds the evidence sufficient, it allows the police, in accordance with the Fourth Amendment, to conduct a "search"—in this case, to tap a phone. The police then implement the tap, typically placing it at some juncture of the phone lines outside the home, unbeknownst to the suspect inside.

Decryption entails more steps, and a greater number and variety of privacy safeguards than phone-tapping. Under the suggested system, when public authorities have specific evidence that a person is suspected of having committed a crime, they would present this information to a court, and if the court found the evidence sufficient, it would issue a warrant allowing the authority to retrieve the private key from the places where it is escrowed. The various escrow agents would verify that the authority has a proper warrant. They each would then provide the authority with a part of the needed key. That is, the authority would have to demonstrate to at least two independent (nongovernmental) agents that a valid warrant has been issued. The retrieved key components could then be reassembled and used to decrypt the particular messages.[39] It seems reasonable to conclude that, if anything, privacy is better protected when public authorities seek to decrypt messages rather than when they are tapping phones.

The main flaw in the individualists' analysis of key recovery is that it presumes that everyone will be treated as if they were criminal suspects. There is neither reason nor evidence to support this assumption. Listening in on suspected criminals—not on those the police declare are criminals, but those the courts have decreed as such—is not the same as eavesdropping on "all free citizens." And it is already routinely and legally carried out. Indeed, if limiting the freedoms of suspected criminals had the debilitating effects that the individualists fear, American liberty and democracy would have been lost long ago.

One might object to the very concept of criminal suspects and argue that unless a person is convicted he or she should be treated the same way as those who are not suspected of wrongdoing. But this is an argument not against key recovery but against a major foundation of our system of justice. Anyone holding this position would also have to object to all the various measures involved in gathering evidence of

criminal wrongdoing, not merely to key recovery. But none of the individualists cited embrace this position—and for good reason. If we were to abolish the category of criminal suspect, we would cripple our capacity to maintain public safety when we ended up either treating all citizens as suspects or treating all suspects like criminals, as totalitarian regimes do. Assume there is credible evidence that John Doe may have committed a crime, but insufficient evidence for arrest and conviction. The public authorities have only three choices: ignore the evidence (let a man who might well have committed a crime run free); act as if the evidence is sufficient (jail a man who may not have committed a crime); or take additional steps to clear up or verify the suspicion.

Democracies have made a special point, from the Magna Carta on, of treating suspects as a special category. To attack key recovery is to oppose, however unwittingly, this critically important principle.

OVERBLOWN ANALOGIES

The debate about the legitimacy of key recovery is not confined to courts of law and law professors. To make their case in other arenas, individualists have employed powerful, evocative analogies. Most of these are similar to the one explored here.

In 1994 Ron Rivest wrote to Dorothy Denning, a supporter of the Clipper chip: "You seem to believe that anything that will 'block crime' must therefore be a 'good thing' and should therefore be adopted. This is not true, even if it is not subject to government abuse."[40] No such belief is in evidence. The argument advanced by Denning and others is not that "anything goes," but that such a measure is justified in light of the scope of the danger posed by terrorists and other criminals, and given the minimal, if any, intrusiveness (compared to phones) introduced by public key recovery.

Rivest continued:

> For example, a system that could turn any telephone (even when on-hook) into an authorized listening microphone might help law enforcement, but would be unacceptable to almost all Americans. As another example, tattooing a person's social security number on his or her but-

> tocks might help law enforcement, but would also be objectionable. Or, you could require all citizens to wear a bracelet that could be remotely queried (electronically, and only when authorized) to return the location of that citizen. There are all kinds of wonderfully stupid things one could do with modern technology that could "help" law enforcement. But merely being of assistance to law enforcement doesn't make a proposal a good thing; many such ideas are objectionable and unacceptable because of the unreasonably large cost/benefit ratio (real or psychological cost). The Clipper proposal, in my opinion, is of exactly this nature.[41]

Analogies of the kind that Rivest employs are indeed powerful. One cannot but at first be horrified contemplating such an intrusion by Big Brother into every home. Upon closer examination, however, none of these analogies hold. Tattooing people, aside from being reminiscent of Nazi atrocities, entails a much higher level of intrusiveness than simply reading messages.

Most important, Rivest—like Froomkin—presumes that the government would in fact listen in randomly on all or millions of Americans' phones, or turn television sets into microphones, rather than merely eavesdrop on those who are criminal suspects. For the latter, the differences between turning an on-the-hook phone into a listening device (a relatively new capability) and surreptitiously driving spike microphones into the walls of the homes of suspected criminals, an act long considered legal by the highest court in the land, are technical and limited in import. The Supreme Court ruled in *Dalia v. United States* (1979) that police, provided they have a warrant, can even break covertly into a suspect's home "for the purpose of installing otherwise legal electronic bugging equipment." The latter category includes not only phone taps but also microphones, tape recorders, and other electronic eavesdropping devices. And these may legitimately be placed in all manner of locations—in lamps, closets, and elsewhere. In short, on closer examination, the far-fetched analogies simply do not hold.

CYBERSPACE ANARCHISTS

In most, if not all, ideological camps there are moderates and there are more extreme advocates. The same holds for various groups of civil

rights advocates, libertarians, and other individualists. According to several accounts, however, the camps of strong cyber-libertarians (sometimes referred to as cypherpunks) are particularly large and dedicated. Cyberspace seems to be the new territory where hyper-libertarians congregate, and the medium on which they pin their hopes for a world free of any government.

Steven Levy described cypherpunks in the pages of the *New York Times:*

> Cypherpunks share a few common premises. They assume that cryptography is a liberating tool, one that empowers individuals. They think that one of the most important uses of cryptography is to protect communications from The Government. . . . The Cypherpunks consider the Clipper the lever that Big Brother is using to pry into the conversations, messages and transactions of the computer age. These high-tech Paul Reveres are trying to mobilize America against the evil portent of a "cyberspace police state," as one of their Internet jeremiads put it. Joining them in the battle is a formidable force, including almost all of the communications and computer industries, many members of Congress and political columnists of all stripes. The anti-Clipper aggregation is an equal-opportunity country club, uniting the American Civil Liberties Union and Rush Limbaugh.[42]

Many cyber-libertarians believe that cyberspace could—and should—be a world free from all government intervention and regulation. Moreover, as the proportion of all communications that are carried out electronically eclipses the older forms of face-to-face communication, so too will we see an increase in the importance of cyberspace.[43] In short, the old dream of the withering away of the state has found a new life on the Internet. In such a world the government would not decrypt messages; it would either not be allowed in or be rendered irrelevant and gradually cease to exist.

Sameer Parekh, addressing a conference sponsored by the libertarian Cato Institute, contended that "the rapid development of strong cryptography is the antidote to the disease of government."[44] And Tim May, a leading crypto-anarchist, writes: "Many of us see strong crypto[graphy] as the key enabling technology for a new economic and social system, a system which will develop as cyberspace becomes more important. At issue is the end of governments as we know them today."[45]

Phil Zimmermann is a leading figure among the strong cyber-libertarians. He defied public authorities by putting his powerful encryption program on the Internet, making it freely available worldwide to all comers, including, of course, criminals and terrorists. Like other cyber-libertarians, Zimmermann views the government as the problem because it is, or may turn into, a tyranny. Zimmermann declares: "When making public policy decisions about new technologies for the government, I think one should ask oneself which technologies would best strengthen the hand of a police state. Then, do not allow the government to deploy those technologies. This is simply a matter of good civic hygiene." Zimmermann acknowledges that blocking the government's endeavors will help criminals, but he argues that this is a cost we must bear—much like the pollution caused by cars—for the liberty such efforts will ensure.[46]

John Perry Barlow, founder of the Electronic Frontier Foundation and a prominent cyber-libertarian, issued the "Cyberspace Independence Declaration," which decries external control of digital communications:

> I declare the global social space we are building to be naturally independent of the tyrannies [that governments] seek to impose on us. [Governments] have no moral right to rule us nor do [they] possess any methods of enforcement we have true reason to fear.
>
> . . . Increasingly hostile and colonial measures place us in the same position as those previous lovers of freedom and self-determination who had to reject the authorities of distant, uninformed powers. We must declare our virtual selves immune to [governmental] sovereignty.[47]

Cyber-libertarians tend to be more than just strong advocates of privacy and freedom; they are often highly suspicious of the government. They believe that the whole institution, not merely some of its acts, is illegitimate and inherently untrustworthy. A rather moderate advocate, Marc Rotenberg, director of the Electronic Privacy Information Center (EPIC), points out that efforts to prevent strong encryption programs from reaching the wrong hands are "naturally viewed with suspicion" by his followers.[48] "You don't want to buy a set of car keys from a guy who specializes in stealing cars," he says. "The NSA [National Security Agency]'s specialty is the ability to break

codes, and they are saying, 'Here, take our keys, we promise you they'll work.'"[49] John Perry Barlow, in his 1992 essay "Decrypting the Puzzle Palace," claimed that "relying on government to protect your privacy is like asking a peeping tom to install your window blinds."[50]

The cypherpunk position is viewed as verging on the "paranoiac." "Because Skipjack [included in the strong encryption provided by the U.S. government] is not open to public review, some people have questioned whether NSA might have intentionally sabotaged the algorithm with a trap door that would allow the government to decode encrypted communications while bypassing the escrow agents."[51] When researchers at the University of California at Berkeley cracked the encryption code used to scramble cellular phones, they believed the government had intentionally weakened the code for surveillance purposes. However, they presented no evidence in support of this claim. In addition, rumors abound in the computer software industry that NSA agents posing as encryption engineers have written elaborate encryption programs to which they secretly have the keys.[52]

Froomkin suggests that the fundamental issues raised by encryption

> revolve around trust: whether citizens should be asked to trust the state with the means of acquiring the citizens' secrets, and whether the community and the state feel they can afford to allow citizens, as well as foreign citizens and foreign states, access to technologies that enhance secret-keeping to the point that police or intelligence agencies might find it impossible to monitor communications or search a computer's hard drive.[53]

My concern is with both forms of trust, and with finding a judicious balance between them. Cyberspace is not extraterritorial. It is subject to the same basic balances of liberty and social order, privacy and the common good, as other areas of social life.

A SERIES OF CONCESSIONS THAT FAILED

Encryption has been around for 4,000 years,[54] but the issues under discussion only recently came into public focus, in 1993, when the government first floated the idea of so-called public (or law enforcement) key recovery. The idea has been to give private parties that wish

to use encryption two choices: (1) use hyper-encryption but provide public authorities with the key (public keys are deposited in a safe place, or "recovered," in contrast to a private key depository utilized by private parties to store spare keys in case they lose a key and are unable to access their encrypted data); or (2) use weaker encryption, without giving public authorities any keys, presumably on the grounds that the government could crack these messages on its own. Basically the choice was either to grant police a peephole for your new steel door or to make it out of glass.

Since 1993 the U.S. government has tried to promote its approach voluntarily, drawing on an odd measure that did not require legislation, namely export controls. The U.S. government decreed that export of encryption must be limited to weak systems and to hyper-encryption that contains a key the government can use.

Although theoretically private parties *in* the United States could build and sell any encryption system, the government hoped at the time that the exportable model would become the standard, because it makes little economic sense to produce different models for export and domestic use. Law enforcement officials would thus be able to decipher messages when appropriate, one way or the other. The government also assumed that the encryption model it provided, equipped with a chip that had a public key in it (known as the Clipper chip),[55] had a stronger encryption program than was otherwise available.

The government approach was widely criticized for curbing American ability to export ("Who would buy such programs?"), for giving itself ready access to encrypted messages, and for other weighty reasons spelled out later in this chapter. The opposition, by American corporations seeking unfettered exports of their encryption products and privacy advocates fearing government eavesdropping, was so intense that the government soon modified its position.

In mid-1994 Vice President Gore wrote to Representative Maria Cantwell (D-Wash.) that the Clinton administration was "willing to engage in serious negotiations leading to a comprehensive new policy on digital privacy and security."[56] However, civil libertarians felt that Gore's letter marked the administration's continuing desire to increase electronic surveillance.

In 1996 software companies were allowed to export somewhat more robust systems, and soon thereafter even more robust ones. Export control was moved from the somewhat strict State Department to the more accommodating Department of Commerce. Suggestions were made that the keys needed to crack messages be moved from a government depository to escrows to be maintained by select private parties, organizations, or trustees to assure users that the keys could not be employed in an inappropriate manner. These suggestions were also rejected by the opposition.

In 1997 a bill was drafted by the Clinton administration that further clarified the limited conditions under which the keys would be released for use by the government and added criminal penalties for those who abused them. The administration also suggested that keys be split among two or more depositories so that no single party could activate them. The bill, like many others, has not been enacted because of strong opposition from libertarians, civil libertarians, and commercial groups.

In July 1998 the Clinton administration announced that it would allow virtually unbreakable encryption packages to be exported *without* the option of key recovery or "backdoor" access, for banks and financial institutions in forty-five countries. According to the new policy, encryption software can be exported to member countries of an international anti-money-laundering accord or to those that have enacted approved anti-money-laundering laws. The software is subject to a onetime review before it can be exported. Nonetheless, a group of software companies, privacy advocates, and libertarians expressed dissatisfaction, calling the government's concession "insignificant."[57]

IN CONCLUSION

"Compromise" is a term that appears often in news reports about encryption.[58] The term is somewhat inaccurate because practically all concessions so far have been made by the government, and yet the opposition still opposes the government proposals. No compromise has been reached with those who campaigned against the revised and diluted law enforcement key recovery systems and have so far succeeded

in blocking them. It is testament to the scope of the opposition that when one of the earlier plans—the introduction of the Clipper chip and export controls—was submitted by the Clinton administration for public commentary, the opposing comments ran 318–2 against it.[59] In none of the cases studied in this volume do we see more forces, or stronger ones, so intensely focused on the real and imagined dangers of overbearing public authorities or so unmindful of the dangers to public safety.

One can readily grant that public authorities in a democracy can abuse their powers, and that a free society requires constant vigilance against such abuses. But our detailed examination suggests that the dangers encryption poses to a free society (not to be confused with an anarchist dream of an ungoverned cyberspace) are particularly limited—compared to phone taps, for instance. Moreover, the dangers to public safety and national security of allowing criminals and terrorists free access to uncrackable encryption are particularly high. It is quite possible that some new technological development may eventually render the whole issue obsolete. The NSA might, for instance, come up with a way to crack encryption without being granted keys. Nevertheless, this examination still stands as a grand illustration of the nature of the arguments advanced by cyber-individualists, and as an indication of their pervasive influence on public policies.