Encryption

Export Controls Harm American Companies
While Failing To Achieve Their Objectives

Introduction

The battle for secure communications is an old one. For millennia people have sought to protect the security of their communications by preventing them from being understood by others who might intercept them. At the same time, others have sought new ways to disentangle intercepted communications and gain access to the information within. Until recently, the running battle between encryption and decryption technology looked likely to continue indefinitely. Although business and governments have developed codes that remain secure for extended periods of time, every code has eventually given way to a solution.

Some people think that technology may have finally produced a winner. The ready availability of massive computing power allows software programmers to use complex mathematical formulae to encode messages. One of the most popular forms of encryption uses the product of two extremely large prime numbers to transform electronic information into what seems like random noise. Cheap computing power allows users easily to encode and decode messages, provided they know the keys on which the coding algorithm is based. Without the keys, other parties must try numbers randomly until they hit upon the right one. Whereas the computer time taken to process messages increases only slightly with the length of the key, the number of random tries needed to guess the key increases exponentially. With a sufficiently long key, modern computers might run for thousands of years without hitting on the right key.\(^1\)

In addition to advancing encryption technology, rapid advances in information technology have increased the importance of electronic communication in both the business and personal worlds. Businesses increasingly are using the Internet and other transmission links as media for conducting business and exchanging valuable information. These networks often contain sensitive business and personal data. Consumers are slowly becoming comfortable about exchanging personal information and conducting financial transactions electronically. The increased use of the Internet rather than of dedicated lines to deliver much of this information makes it even more important that its security rely on encryption rather than on restricted access to physical locations.

Information security is a double-edged sword, however. Information can be harmful as well as beneficial. In particular, law enforcement and national security agencies are increasingly worried that criminals and terrorists will use encryption to plan and execute crimes and launder money. Although these agencies have the ability to intercept messages in transit or when it is stored, wiretaps and subpoenas

\(^1\) Combination safes provide a valuable analogy. Adding one digit to the correct combination has only a marginal effect on the cost or convenience of the lock. But it increases the number of possible combinations by a factor of 10. But significantly, few burglars open a safe by trying every possible combination until they get the right one.
are of little use if the information they contain is encoded to resemble gibberish. Widespread use of encryption would diminish the agencies’ ability to conduct surveillance on suspected criminals.

During the last seven years, the Clinton Administration has fought a protracted battle to prevent the spread of encryption technology. This battle has been justified largely on law enforcement grounds. Administration officials routinely cite the possibility of terrorist bombings, kidnappings, and child pornography rings as justification for making sure that encryption technology does not advance beyond their ability to gain access to the underlying information.2

This report does not argue that these fears are groundless. It does, however, argue that the Administration’s efforts are almost certainly doomed in the long run. The real effect of the government’s policy is merely to delay the deployment of encryption technology, not to transform it. This delay has significant costs, however. One of the most serious costs is the loss of export markets to U.S. makers of encryption software. This loss in turn weakens domestic law enforcement agencies by transferring market share to foreign companies that have fewer incentives to cooperate with them.

## Current Restrictions on Encryption Technology

There are now no restrictions on the domestic use of encryption technology.3 Instead, most of the government’s efforts have focused on controlling the export of encryption software and on using its purchasing and persuasive powers to influence the development of commercial software products. The Administration classifies encryption software using keys of more than 40 bits as a munition under the Export Control Act. Although the act has expired, the Administration continues to enforce these controls using general emergency powers granted to it by the Congress. In the beginning, these controls were unrealistically harsh. At one point people traveling on business were technically committing a felony whenever they took their portable computers abroad since the computers often were preloaded with restricted encryption software.

In recent years the Administration has slowly liberalized these controls. Authority to grant export licenses has been transferred from the State Department to the Commerce Department, which is generally viewed as more sympathetic to the business community. Controls have been removed for keys of 56 bits or longer, subject to a one-time review, provided the manufacturer is developing a key escrow system. Most recently, the Department has removed limits on the strength of software exports to financial customers and to the overseas subsidiaries of domestic companies. The latter concession allows U.S. companies to protect their global communications with a single encryption package using U.S. software.

In addition to export controls, the Administration has attempted to influence the domestic use of encryption software. Rather than prohibit the use of encryption software, the Administration has sought to use its market power and the export controls to encourage software manufacturers to build a key escrow system into their programs. With key escrow, either the government or a third party would hold the keys needed to decode messages. Law enforcement would be able to get access to these keys with a warrant. The grounds for obtaining a warrant would presumably be similar to those needed for a wiretap or search warrant.

Opposition to encryption controls is divided into two groups, each motivated by a different primary concern. Although the two groups agree on many points, their positions differ, especially with respect to the concessions they would make to meet the concerns of law enforcement. The business community is primarily concerned with the loss of export markets and the dangers of reduced security for electronic commerce and company communications. They view the current export controls as slowing, but not stopping, the widespread use of encryption software. In the meantime, U.S. software developers are prevented from using their technological lead to serve these markets. Instead, foreign companies have used the time to develop competing software programs. The business community does not necessarily have a philosophical objection to government controls, provided they do not seriously slow the spread of encryption for legitimate uses or disadvantage U.S. companies. But it argues that export controls are unlikely to have a lasting effect on the use of the technology, especially when few governments are willing to follow the Administration’s lead. Other businesses are primarily concerned with the security of their internal and external

---


3 Most arguments about the ineffectiveness of encryption policy apply equally to domestic and export controls. The Administration has not advocated domestic restrictions. Law enforcement agencies have accepted this approach on the condition that the private sector cooperate in developing alternative policies to address law enforcement concerns. The agencies have reserved the right to press for domestic controls at a later date should voluntary actions be insufficient.
communications or with the effect of encryption policies on public confidence in electronic commerce.

A number of groups oppose any controls on privacy and Constitutional grounds. These groups are deeply suspicious of the government's desire to have its agents intercept and decode private messages. If the encryption keys are entrusted to the government's care, the need to get a warrant before they are used may be honored only when evidence is needed for a criminal trial. At other times, individual agents may decide to use warrantless searches to track suspected criminals or to gather information for general use. This group tends to view encryption controls as free speech protected by the Constitution. They strongly oppose any attempt to restrict the use of encryption or to require the use of key escrow systems. These groups are less concerned about the impact of government policy on business.

One of the cardinal rules of public policy ought to be that a given policy must have a reasonable chance of success in order to be justified. By this rule, the Administration's current policy, even in its weakened state, cannot be justified. Regardless of the merits of encryption controls, the Administration's approach is likely to fail for five main reasons:

1. The Benefits from the Widespread Use of Encryption Technology Outweigh its Costs
2. A Workable International Key Recovery Agreement Would Be Difficult to Implement
3. In the Long-Run, Export Controls Cannot Work Without Effective Domestic Controls
4. Immediate Key Recovery May Be Impossible at High Levels of Security
5. Encryption Technology Does Not Represent a Significant Threat to Law Enforcement

Each of these reasons is fatal. Since the policy is unlikely to meet its goals, there is no corresponding benefit to outweigh the significant costs of the export controls.

**Why the Administration's Encryption Policy Will Fail**

**The Benefits From the Widespread Use of Encryption Technology Outweigh its Costs**

The Administration's position is built on the implied assumption that widespread use of encryption technology will impose significant costs on society unless law enforcement officials maintain an ability to gain instant access to plain text communications. If this assumption is false, then the current export controls impose a net cost on society.

The idea of every person being able to communicate with many others in total security can give one pause, until one realizes that the government's ability to intercept communications has always been limited. Secure encryption can help criminals and terrorists escape detection. Law enforcement agencies routinely point to this possibility to justify government restrictions. There is no doubt that such cases will arise. But when they do, law enforcement has many other tools that it can use to track and prosecute criminals. These tools are continuously being strengthened, most recently with calls for a centralized program within the Federal Bureau of Investigation to coordinate decryption efforts. Most criminals do not use encryption. In the few cases where encryption is used, law enforcement officials have usually been able to recover the plain text.

Although encryption helps criminals, it also helps ordinary citizens in two ways. First, any attempt by the government to limit the strength of encryption technology or to mandate key recovery increases the chance that individuals other than law enforcement officials will intercept legitimate communications. Crime can be furthered in two ways. One is by allowing criminals to use encryption to avoid government surveillance. The other is by weakening the security precautions that prevent criminals from breaking into legitimate communication networks. Federal policy assumes that the natural conflicts between these two possibilities can be avoided by creating security systems that are walled off against everyone except the government. Such a perfect outcome is unlikely. Instead, efforts to restrict the use or development of encryption technology are likely to increase the vulnerability of these networks to hackers.

A good example is the present state of security surrounding analog wireless telephones. When these phone systems were first introduced, the government pressured manufacturers to avoid building encryption technology into the networks. As a result, telephone conversations can easily be intercepted with relatively unsophisticated equipment. Similarly, researchers recently cracked the encryption code used by some digital phones. In doing so, they found evidence indicating that the code had been intentionally weakened to ease government access.¹

---

¹ At least three federal court cases are testing this argument by challenging the government's prohibition on putting source code on the Internet. A court of appeals recently ruled that the export controls violated the plaintiff's First Amendment protections. In the other two cases, lower courts in other circuits found that the controls constituted a reasonable regulation of the code's function as opposed to its content.

---

In some cases the intentional weakening of security systems has benefited law enforcement. The Kurdish terrorist Abdullah Ocalan was captured reportedly after U.S. officials in Kenya intercepted his telephone conversations. But the lack of security has much larger private costs. In 1997, a Florida couple taped a private conversation between Republican congressmen, including then-Speaker Newt Gingrich and their staffs. Nor are the costs of reduced security limited to personal embarrassment. Telephone fraud involving cellular phones is widespread. The annual cost to telephone companies of unauthorized and fraudulent calls runs in the billions of dollars.

Not all of these costs are private. The President’s Commission on Critical Infrastructure Protection recently issued a report pointing out the dangers of physical and cyber attacks to the nation’s infrastructure. Since then the Administration has set up a National Infrastructure Protection Center to coordinate public and private efforts to increase security. Computer security consists of a web of tools and practices. Strong encryption must be one of them.

A recent report by a committee of the National Research Council recognized the benefits of encryption when it concluded that:

... [C]urrent U.S. policy should be changed to promote and encourage the widespread use of cryptography for the protection of the information interests of individuals, businesses, government agencies, and the nation as a whole, while respecting legitimate national needs of law enforcement and intelligence for national security and foreign policy purposes to the extent consistent with good information protection.

By itself, this recommendation could cover a variety of policies, including the Administration’s current approach. But the committee specifically stated that:

... [C]urrent national cryptography policy is not adequate to support the information security requirements of an information society. Indeed, current policy discourages the use of cryptography, whether intentionally or not, and in so doing impedes the ability of the nation to use cryptographic tools that would help to remediate certain important vulnerabilities.

... [W]idespread commercial and private use of cryptography in the United States and abroad is inevitable in the long run and ... its advantages, on balance, outweigh its disadvantages.

The costs of reduced security are often harder to measure and less dramatic than the threat of a terrorist bomb, but they are just as real and they should be taken into account when setting encryption policy. For example, it is possible that encryption controls could actually increase the damage from a terrorist attack by weakening the protection of communications systems. With the combined growth of telecommunications and computer technology, an increasingly large part of the nation’s infrastructure now depends upon complex information networks. Yet at the same time as the Administration seeks to strengthen the security of electronic systems, its export controls delay the spread of technology that would make it more difficult for individuals to break into these systems.

There is a second way in which the spread of encryption technology can enhance national security. Giving citizens in other nations the ability to communicate securely without government oversight can strengthen the security of the United States by promoting economic and political democracy abroad. Although we cannot prevent governments such as China from outlawing the use of encryption technology, we can ensure that such technology is easy to obtain over the Internet and encourage its use by dissidents. Because it is extremely hard to control access to and use of the Internet, the availability of encryption software will increase individual freedom regardless of government policy. The Internet has already played an important role in organizing democratic efforts in both Eastern Europe and Asia, allowing individuals to obtain information and coordinate plans without having to depend on government agencies such as the press or mail service. On a global level, encryption is far more likely to protect individuals from repressive governments than it is to aid terrorists seeking to harm democracies. This in turn weakens the power of states whose interests are fundamentally opposed to ours.

The benefits of increasing the security of information networks and of private communications

---


---

8 Ibid., pp. 6, 13 (italics added).
between individuals in repressive societies are different. But together they legitimize the contention that unfettered encryption may be a net benefit to society, not a threat. While this contention can be debated, it does not deserve the summary dismissal that law enforcement typically gives it. And law enforcement's claims that we can maintain those benefits while still controlling the use of encryption should be viewed with strong suspicion, given the government's effort to weaken the security of cellular transmissions. If the benefits of encryption outweigh its costs, it is likely that software developers and users will continue to use strong encryption despite government attempts to stop them.

A Workable International Key Recovery Agreement Would Be Difficult To Implement

One of the strongest arguments against unilateral export controls is that, although they harm U.S. business interests, in the end they accomplish very little in terms of foreign policy. Unless other nations are willing to follow America's lead, foreign customers who are denied access to U.S. products can often purchase identical products from Europe, Japan, or any other nation that produces it. Many governments are not willing to restrict the export of encryption products from their countries. As a result, strong encryption programs are widely available from foreign manufacturers. Finally, even if a coordinated export control program could be worked out, there are serious doubts about the workability of any international key escrow system.

Over the past several years, foreign software companies have developed encryption packages that rival those offered by U.S. companies. In some cases, these efforts have been aided by investments by American companies seeking to retain a role in global encryption markets. The Administration has attempted to negotiate with other nations to limit the spread of encryption technology. An international agreement is necessary because export controls on the spread of American software cannot accomplish their goal as long as equivalent programs are available from German or Russian software companies. Just as important, the powers of law enforcement are compromised if other nations let their citizens use unrestricted encryption.

The European Commission has rejected U.S. arguments and called for unlimited, market-driven use of encryption in the European Union. Although some European countries such as France and Great Britain impose domestic controls on encryption software, others do not. The Commission's policy paper indicates that strong encryption products without key escrow are likely to be used in at least some countries. This will place pressure on countries that require their citizens to use encryption programs that ensure government access.

The Administration recently claimed success when some developed countries agreed to review their domestic laws on encryption as part of the Wassenaar Arrangement. This agreement did not do much to address the Administration's central problem, however. First, several states that are developing encryption technology, such as Russia and China, are not parties to the agreement. Second, even those parties that are part of the agreement are unlikely to limit exports as a result of it. They merely promised to examine their laws regarding encryption use and exports. Individual countries will still need to pass domestic legislation before the agreement has any real effect. Since the market incentives for them to continue permitting the export of encryption technology have not changed, it is unlikely that they will follow the United States' lead in export controls.

Since the agreement did not really represent a consensus that current export controls are too loose, it is not clear that these laws will be passed. It would probably be more accurate to say that Wassenaar agreement was an agreement to continue disagreeing about international controls. In the end, other nations are unlikely to follow the U.S. lead and give up on export sales. This is partly because the Europeans and Japanese tend to take a more pragmatic view of dealing with unsavory governments. But economic considerations also matter. The sale of encryption software often serves as an entry point for handling a company's broader communication needs such as enterprise-resource programs. With the U.S. having abandoned its lead in this aspect of software technology, foreign governments are unlikely to resist taking advantage of this chance to gain a competitive advantage over American companies.

There is a more serious objection to the concept of an international agreement, however. It is difficult to see how such an agreement would work without infringing too severely on national sovereignty. The goals of American law enforcement officials are not really met if terrorists move their

---


10 This agreement occurred in the context of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual Use Goods and Technologies that replaced the Coordinating Committee on Multilateral Export Controls (COCOM) as the coordinating organization among Western nations for munitions controls.
communications center from the United States to Germany. The objective of law enforcement and national security agencies presumably is to be able to decrypt any message sent from any location. This can be done only if other countries restrict the use of encryption within their borders. So far few nations have done so. Yet, if any major nation allows the development and use of strong encryption without a mechanism such as key escrow to meet law enforcement needs, users in other countries are likely to press their governments for permission to use it. Even if key escrow is used, the keys must be made quickly available to U.S. officials.

Several solutions are available, but all of them present serious policy problems. The first would be to mandate that software packages make their encryption keys available to each government. Besides increasing the logistical complexity imposed on software manufacturers, such a policy would dramatically increase the probability of unauthorized eavesdropping and would mean that vital communications could be subject to prying by any of several governments depending upon their own domestic laws. American companies and individuals are likely to resist escrowing their keys with a French or German authority. The danger becomes even greater when the programs are used to communicate with Russian or Chinese parties whose governments are likely to want similar access to encryption keys.

An alternative to requiring escrow in each country is to require it in only one place. This also presents problems. Would U.S. law enforcement officials be content if they were forced to issue a subpoena against a German escrow agent every time they needed to decrypt communications encoded with German software? Given recent problems extraditing known killers from allied countries such as France and Israel, it is easy to foresee instances in which such cooperation is either difficult to obtain or occurs too late to be of help. Obtaining cooperation from countries such as China and Russia will be even harder. These problems are different, but no easier when U.S. software is used.

While we may imagine U.S. officials sharing access to encryption keys with German officials, few would support making them available to Chinese officials who may be trying to enforce their domestic laws on the use of the Internet. Yet if we cannot allow Chinese officials to use an American key escrow system, they will certainly not let us use their system. Unless they are guaranteed access to the escrowed keys of software sold by others, nations have little incentive to control exports of encryption software produced by their own companies, even if they do not provide for key escrow.

In the Long Run, Export Controls Cannot Work Without Effective Domestic Controls

Strong encryption systems are readily available over the Internet for anyone to use. For example, a software package named Pretty Good Privacy uses 128-bit encryption. A version of it can be downloaded for $39.95 at http://store.mcafee.com.

Export control laws do not restrict the domestic development or use of new technology. There are currently no domestic controls on the use of encryption technology within the United States. This severely weakens the effectiveness of export controls, however. Unlike missiles or high-end computers, encryption software can easily leave the United States despite the best government precautions. A foreign national can purchase a software program in the United States and then carry it abroad in a compact disk with virtually no chance of detection. Or he can simply e-mail it to a foreign location. Once abroad, unlimited copies can be cheaply made.

A trip to the United States may not even be necessary. Software developers can simply place their programs on the Internet where they are available to everyone. The Administration has argued that publishing executable code on the Internet constitutes an export of the technology, since the code can be downloaded overseas. This position raises serious First Amendment issues, since the publishing can occur in the context of academic and business activities that are normally protected as free speech. The federal courts have split on the constitutionality of the Administration's position. A definitive ruling against the government would severely weaken its ability to control the spread of encryption technology.

Even if the Internet is not used to send encryption technology abroad, widespread use of encryption technology within this country poses a challenge to the wisdom of export controls. Export controls do not address law enforcement's desire to decrypt the communications of criminals who plot their activities within our borders. And, as stated above, export controls are ineffective if foreign criminals use non-U.S. software that does not provide for key encryption. If law enforcement is really serious about the need to decrypt all communications, wherever they occur, it will eventually be necessary to outlaw the domestic use of encryption technology that does not provide for some type of key recovery. Such laws will be needed both in the United States and in other countries. There is a good argument that in the United States citizens have a First Amendment right to use strong encryption without giving the government the ability to listen to an encrypted communication.
Some law enforcement officials have acknowledged the need for domestic controls. Louis Freeh, Director of the Federal Bureau of Investigation, has stated that he favors mandatory key recovery in the United States, although he recognizes that it is politically infeasible at present. The Administration has been less forthcoming, merely stating that it has no intention of seeking domestic controls at this time. Instead, advocates of domestic controls seem to hope that the government can use its market influence and powers of persuasion to convince the manufacturers of commercial encryption software to build access into their systems without any legal mandate. Public anxiety over the identification features of the new Pentium III computer chip shows that public resistance to such access is likely to be high. As long as they are given the choice, companies are likely to prefer systems without key escrow.

Law enforcement’s logical need for domestic controls to accomplish its stated objectives makes it harder to find a compromise over encryption policy. Many opponents of the Administration’s position are convinced that law enforcement officials will eventually want access to all domestic communications. In the past, the Administration has sought to portray fear of domestic controls as alarmist and irresponsible. But any compromise on export controls would be a first step in this direction. Indeed, Director Freeh’s statement favoring domestic controls contradicts many previous assurances by law enforcement officials. Given other recent abuses of power by law enforcement officials, the distrust of many encryption supporters is understandable.

Immediate Key Recovery May Be Impossible at High Levels of Security

The price of the computing power needed to process encryption algorithms will continue to fall rapidly, allowing encryption software to become even more secure. The best systems now triple encrypt messages before sending them and generate a new key for each message. This places heavy demands on any system meant to give law enforcement the ability to decrypt messages instantly. Law enforcement officials have made it clear that they are not content with the ability to decrypt slowly stored records of the type needed to gather evidence against a bank charged with tax evasion or a suspected child pornographer. Officials also want the ability to decrypt messages as they are being transmitted. This power would be especially important in trying to stop an imminent terrorist threat or in dealing with an ongoing kidnapping.

It is not clear that the technology to do this either exists or can be developed and used without compromising security. In the case of analog cellular phones, law enforcement officials solved this problem by pressuring manufacturers to build an extremely low level of security into their systems. This made it easier for law enforcement to listen in, but also increased the system’s vulnerability to fraud and eavesdropping. The costs of this lower level of security were probably much greater than its benefits. Given the increased importance of the information infrastructure, a lower level of encryption security should not be imposed on digital communications.

But despite their assurances, it is doubtful that officials can develop a workable system for providing immediate recovery for strong encryption systems. Even proponents of the Administration’s efforts to limit encryption technology admit that immediate key recovery poses several difficult challenges. Unless key recovery proves to be workable in practice, law enforcement’s current efforts seem futile. If the technology always remains one step ahead of the government’s ability to control it, the only solution may be to restrict use to those methods with which the government feels comfortable. Business communications would then be more vulnerable than they need to be.

The Administration has argued that the business community should share its interest in developing a workable key recovery system. In some areas, the government’s interest does parallel that of private users. Many businesses will want to retain the ability to decrypt records for audit purposes and to recover lost encryption keys. Managers also recognize that the interests of employees sometimes diverge from those of their employer and will therefore want to maintain some supervisory capability over rogue or disgruntled employees. As long as these capabilities exist within a firm, law enforcement can access them with a subpoena.

The business community’s need for key recovery is not likely to cover the full range of its communications with other parties, however. Specifically, businesses are more likely to value the ability to reconstruct records and communications than to intercept them on a real-time basis. Yet, the most powerful scenarios that law enforcement officers use to justify restricted encryption require the ability to decrypt communications as they are occurring. Moreover, the most dangerous criminal activities are not likely to occur within the institutional setting of an established business that is willing to cooperate with law enforcement in order to protect its broader interests. As a result, the business community is largely powerless to provide the government with
the type of access to the unencrypted messages it most needs.

Because communications involving illegal activity usually occur outside normal business contexts, in order to meet its own goals, law enforcement must possess the ability to intercept and decrypt instantly any message between any two parties anywhere. Even ignoring jurisdictional disputes when communications cross borders, this presents an enormous logistical challenge. Technology now allows messages to be encrypted cheaply with three or more keys of unlimited length, with each key generated randomly and used only once. With billions of messages moving back and forth every day and traveling different routes during each communication, it may not be possible to provide immediate key recovery for any one selected series of conversations at an acceptable price. The problem is far different in nature than it is for cellular phones where, by weakening the overall security of the system, law enforcement and others can monitor transactions in an area with little more than a receiver.

It may not be possible to work out all of the problems associated with immediate key recovery to the Administration's satisfaction. The Administration has attempted to set up such a system to handle intergovernmental communications without any noticeable success. If a key escrow system is infeasible, then either the Administration's attempts to help law enforcement must fail, or the Administration must seek further controls on the technology. It is therefore legitimate to ask whether the Administration will seek to restrict the strength of encryption technology. Any attempt to do so would increase the vulnerability of communications to illegal activity.

Encryption Technology Does Not Represent a Significant Threat to Law Enforcement

Export control laws are having an important effect on domestic companies in the form of lost revenues and reduced security. As usual, however, the ultimate effect of future developments in encryption is likely to be much less significant than either side believes.

Completely secure encryption has always been difficult to achieve. Although modern programs promise to make decryption mathematically impossible, the history of encryption is filled with supposedly unbreakable systems that were later shown to contain fatal flaws. Even today, the most sophisticated systems are periodically found to contain problems. Programs that were considered unbreakable a few years ago have gradually succumbed to a combination of cheaper processing power and flaws in their programming.

The current approach to encryption is probably much more vulnerable than we now think. For one thing, encryption often is only as valuable as the comprehensive security system surrounding it. If other security precautions such as passwords and security clearances are not followed, encryption may be of little use. It is of little value to encode the transmission of a sensitive business report if the employee then prints out a plaintext version and leaves it in the cafeteria.

The abilities of U.S. law enforcement agencies also should not be underestimated. Surveillance by national security and law enforcement officials is far more prevalent than most people assume. Agencies such as the National Security Agency and the Federal Bureau of Investigation will continue to possess superior human and physical resources. In addition, they have access to the advice and assistance of domestic software developers who are willing to help in selected cases. These resources are so strong that many observers believe that most strong encryption no longer poses a serious threat to the government's ability to monitor communications.

Even without export controls, most electronic communications will continue to be accessible to the government with a valid court order. Most criminals do not encrypt their communications. And even the most sophisticated criminal will have to engage in actions that law enforcement officials can track. Any transactions with a legitimate business will generate records that can be subpoenaed. As a result, the results from removal of legal constraints on the use and export of encryption software will not be apocalyptic.

Regardless of the development of encryption technology, the cost of occasional criminal activity, whether it is due to the use of encryption to hide terrorist activity, or the lack of security around an important information grid, is likely to be relatively minor when viewed in terms of the national economy. The cost will certainly be less than that currently imposed by unwise government legislation in a broad range of other areas.

13 One of the world's top cryptographers recently announced the design of a machine that in theory could quickly unscramble cryptographic systems with keys of 512 bits or less. "Israeli Scientist Reports Discovery of Advance in Code Breaking," The New York Times, May 2, 1999, Section 1, p. 37.
The costs of government controls also should not be overstated. The primary objection to such controls is that, in the long run, they are ineffective, not that they impose large costs on the economy. In most instances, the need of business and individuals to communicate with each other will continue to outweigh any fears that the government or others will listen in. These needs continue to drive the widespread use of credit cards and analog cellular phones in spite of the ease of fraud.

Given the relatively low economic consequences, it may be hard to understand why this issue has been so contentious. If most of the points made in this report are correct, then the Administration’s approach is likely to continue imposing costs on the software industry and other businesses with no hope of accomplishing the goals that law enforcement thinks are so important. The continuing press of technology will only worsen the position of law enforcement. Meanwhile, businesses will continue to see export markets slip away. The ineffectiveness of current policy is not the fault of those who oppose the Administration. It is inherent in the technology.

A second reason for skepticism in the business community is that the Administration has always felt free to change its position without clearly spelling out how that position will help it obtain its ultimate goals. Over the past seven years the government has been forced closer and closer to the business community’s position without receiving many concessions in return. The reason is that these retreats have always been tactical ones, forced by the technology rather than the politics of the issue. The Administration has never explicitly stated whether, and to what extent, First Amendment and business security concerns compete with, or outweigh, law enforcement concerns. Without a firm understanding on these issues, it is difficult to discuss the remaining issues. And the continuing suspicion that the Administration will eventually seek domestic controls gives credence to the claims of the free speech community that the government’s attempts at accommodation are tactical and eventually will be reversed.

**Encryption as a Free Speech Issue**

Individual rights and government powers are always in a delicate balance. Advances in encryption technology have upset this balance by threatening to make existing policies obsolete. Law enforcement officials often argue that they are merely trying to restore the original balance struck by existing wiretap laws. They deny that domestic controls would represent an expansion of government powers. Existing laws allow courts to authorize officials to subpoena records and listen in on conversations in their unencrypted form. Although this power applies to encrypted messages, it is of little use since the intercepted messages are unintelligible. Officials therefore claim that encryption weakens their current access to plaintext communications and that a key escrow system is needed to restore the balance. But this argument confuses the extent of the government’s power with its willingness to obtain a court order prior to using those powers.

Encryption is just one way in which technology is altering the balance of power between the individual and government. Although it may be wise in order to restore the previous balance between the state and individuals, mandating key recovery for domestic communications would in fact represent an expansion of the government’s power. Individuals and businesses now have the right to use any encryption technology they wish within the United States. This right has assumed new meaning given the growing strength of computer technology and is slowly placing more power and freedom in the hands of individuals. If the government at some point restricts the use of encryption technology, this change in policy would obviously be an extension of its power.

The existing export controls also represent an expansion of government power. When the government first claimed the ability to read a suspect’s personal diary and to require that suspect to submit to a blood test, these were both viewed as important expansions of its power deserving careful judicial consideration of the benefits and costs of such an expansion. In both cases, the government conceded that it would normally need a court order before it could compel the evidence. At the time, few people confused the Fourth Amendment issue of whether a court order was needed before the government exercised its power to search with the separate issue of the extent of its ability to search. In an extreme case, if some day the government sought to revoke the attorney/client privilege, but only on a showing to the court that the revocation would produce material evidence that was otherwise unavailable to the prosecution, most people would view the attempt as significant extension of the government’s power. The mere fact that the government is required to obtain a court order before gaining the ability to decrypt a message does not negate the fact that its ability to compel the keeping and transfer of keys diminishes the freedom that technology otherwise gives individuals. This expansion of power may be necessary to keep up with technology. It may even be wise. But it is still an expansion.
The issue of whether the government is seeking additional powers, of course, does not determine whether those powers are wise. It might be wise to control the use of encryption software if controls were technologically feasible and their benefits outweighed their costs. But there are still many unanswered questions about the workability of the government's position, especially if one rules out domestic controls. The Administration would almost certainly be better off if it encouraged the use of this new technology to protect American business, to enhance U.S. exports, to increase the individual freedom of foreign citizens subject to repressive governments, and to maximize cooperation between law enforcement officials and the U.S. companies developing the technology.

**Conclusion**

Despite the differences between the business and free speech communities, opinions on encryption ultimately depend on how one balances individual rights and the needs of law enforcement. It is probable that if the Founding Fathers had lacked the wisdom to add the Bill of Rights, concerns for social order and law enforcement would prevent us from enacting anything so bold today. Since rights are difficult to win but easy to lose, they must be guarded zealously. Looking forward, the fear of lawlessness is easy to magnify; the benefits from an expansion of freedom are uncertain. Only by looking back at over 200 years of history and seeing that we have seldom come to regret the growth of individual liberty, one can be complacent that the spread of encryption will not mean the end of social order.

This report was prepared by
Joseph V. Kennedy
Attorney/Economist

Further information on this subject may be obtained by contacting him at 703/841-9000
MANUFACTURERS ALLIANCE/MAPI COUNCIL PROGRAMS

A major part of the overall Alliance program is the work of its councils. Presently there are 35 active councils composed of some 2,000 executives of member companies. These groups have been organized in response to the need for seminar-like groups to meet and discuss challenges and problems in such areas as strategic planning and development, financial management, engineering and technology, global business management, law, marketing, investor relations, manufacturing, human resources, public affairs, government contracts, purchasing, information systems management, logistics management, product liability and product safety, environmental management, risk management, quality, taxation, and general auditing. Membership on Alliance councils is by invitation. Each council meets twice a year, in the fall and in the spring. Council members themselves make presentations, describing recent challenges, projects, and successes. These presentations are followed by candid question-and-answer periods. A business outlook discussion or a wide-ranging roundtable deliberation on items of immediate concern are featured segments at each meeting. The mission and program for several of our councils are set forth below.

INFORMATION SYSTEMS MANAGEMENT COUNCIL

Purpose
The Council's objectives are as follows: (1) to provide a forum for information systems executives to explore all aspects of information management; productivity and quality improvement; delivery of timely and cost-effective data and communications solutions; safeguarding company information from damage or misuse; supporting business processes; and, generally, meeting customer expectations; (2) to promote the exchange of experiences and ideas among information executives representing a broad cross-section of manufacturers; and (3) to serve to the extent appropriate as a clearinghouse for state-of-the-art knowledge concerning member companies' ISM activities.

Program
Meeting agendas for the Information Systems Management Council are designed to address the broad spectrum of issues that confront executives who are charged with managing the information resources and requirements of manufacturing firms. Subjects covered at recent meetings include the following: Benefits of Integrated Manufacturing Systems; Organizing for a Successful ERP Systems Implementation; Client/Server: Approaches and Experiences; Using Year 2000 as a Down Payment To Replace Legacy Systems; Experience in Developing an Automated Customer Service System; The Process of Implementing Integrated Manufacturing Applications; Integrating Computer-Aided Design and Process Planning; Case Study: Experiences With Peoplesoft; Outsourcing Mainframe Services; Recruiting, Training, Motivating, and Compensating IS Personnel; Developing a "Knowledge and Learning" Technology Strategy; Designing and Implementing a Worldwide IS Strategy; Developing a Corporate Internet and Intranet Policy; and Managing Telecommunications Outside of the United States.

For additional information or an invitation to attend an upcoming meeting, please contact:

Frank Holman
Vice President and Secretary and Staff Director
to the Information Systems Management Council
Manufacturers Alliance/MAPI
1525 Wilson Boulevard, Suite 900
Arlington, VA 22209
703/841-9000

LOGISTICS COUNCIL

Purpose
The Logistics Council is still relatively new and growing. The Council takes a broad view of an increasingly important function within manufacturing companies. This is necessary because the logistics function differs widely among our members, ranging all the way from purchasing to distribution. Since logistics is still a rapidly changing field, much of the Council's time is devoted to discussions of its scope and potential within different firms. To date, the Council's agenda has looked at three major areas:

1. Supply chain management
2. Management of the Production Flow
3. Dealing with the additional complexity introduced by outsourcing and strategic partnerships

Program
Presentations discussed by the Council during the last year include: Using Logistics as a Core Competence; What Do We Know About Logistics?; Back-to-Order: An Antidote for Brand Multiplicity; Decentralizing in a Centralized Organization; Supply Chain Management for Electric Utilities; Supply Chain Integration: Suppliers, Customers, and Third Parties; Supplier Relationship Strategies; Supplier-Managed Inventory Communication and Trust; Trends in Carrier Payment Systems and Technologies; Logistics — A Core Competency; Using Strategic Alliances To Improve the Business; Optimizing Warehouse Capacity; Implementing Global Logistics Across Geographical Locations; Adopting Supply Chain Management: Lessons Learned; and European Logistics.

For additional information or an invitation to attend an upcoming meeting, please contact:

Joe Kennedy
Attorney/Economist and Staff Director to the Logistics Council
Manufacturers Alliance/MAPI
1525 Wilson Boulevard, Suite 900
Arlington, VA 22209
703/841-9000