THE CLIPPER INITIATIVE

All Americans have a Right to Privacy!
But Key Escrow Won't Help

Stephen T. Walker[1]
Trusted Information Systems, Inc.

August 31, 1993

1. Summary

On April 16, 1993, the President announced "a voluntary program to improve the security and privacy of telephone communications while meeting the legitimate needs of law enforcement."[2] This announcement contains the very strong statement that:

> "The Administration is committed to policies that protect all Americans' *right to privacy* [emphasis added] while also protecting them from those who break the law."

The announcement describes a new encryption algorithm that is "more powerful" than many in commercial use today while preserving "the ability of federal, state, and local law enforcement agencies to lawfully intercept the phone conversations of criminals" through the use of a "key-escrow" system.

This paper summarizes my review of the information presented to the Computer System Security and Privacy Advisory Board (CSSPAB) in public testimony and related publicly available information concerning the President's "Clipper Chip" Initiative.

Based on this review I have concluded that:

- Key escrow technology will NOT protect Americans "from those who break the law."

- For Administration policies to "protect all Americans' right to privacy," the Administration will have to acknowledge the worldwide availability of good quality cryptography and stop denying Americans the use of technologies that are freely available to others in the name of protecting us "from those who break the law."

---

[1] This paper represents my personal opinions and not necessarily those of any organization with which I am affiliated.

[2] White House Press Release, April 16, 1993.

The real issue confronting us in the President's Clipper Chip Initiative is obtaining an appropriate balance between:

- legitimate law enforcement and national security concerns with intercepting communications that are not in the best interests of the U.S., and

- legitimate concerns with protecting U.S. Government and commercial sector sensitive information and preserving the U.S. economic position.

For too long, the law enforcement and national security interests have controlled the dialog in this debate through their special positioning in the Executive Branch of the Government. Now with advances in technology and worldwide availability of cryptography threatening to impede the ability to easily listen to others, these agencies are proposing potentially highly invasive measures that have little prospect of improving law enforcement and national security intercept capabilities, while having a significant negative impact on U.S. commercial capabilities and interests.

Meanwhile, requirements to protect U.S. Government and commercial sensitive information and maintain U.S. strength in the computer industry remain restricted without a voice in the debate.

While there may be a strong desire to slow the erosion in our technical communications intercept capabilities, this paper will show that the new key escrow approach will have little positive impact because it will see little use beyond the government.

However, if the Administration were to acknowledge today's worldwide availability of good quality encryption capabilities, such as the Data Encryption Standard (DES), our Government and commercial interests in protecting U.S. sensitive data would be vastly improved. In so doing, our ability to intercept others could be marginally hurt, but many feel the gains outweigh the losses.

We must have a balanced review representing both sides of this national dilemma. Such a debate cannot occur exclusively within the Executive Branch of the Government because of its close affiliation with the law enforcement and national security communities and the absence of any effective representation for U.S. commercial interests.

The Congress is the only organization that represents all constituencies affected by such a debate. In the interest of reaching a fair and timely resolution of this national issue, I strongly encourage the Congress to act swiftly to establish a national policy regarding the use of cryptography to resolve this dilemma and clarify all Americans' right to privacy.

2. Background

In the fall of 1992, AT&T announced a telephone security device that would provide high quality security using the DES algorithm to protect the public's sensitive phone calls.[3] Orders were taken for delivery in early 1993. When the devices arrived, purchasers were told they were only "on loan" and would be replaced by a "better" device in "April 1993."

According to Dr. Clinton Brooks of NSA, AT&T came to NSA asking if they should use DES in these devices.[4] NSA realized that if it did not want DES to become widely used in such devices, it would have to accelerate the availability of technology it already had under development (now known as Clipper) that would give higher security than DES but with key escrow[5] capabilities to protect the interests of the law enforcement community. Apparently, AT&T decided to go along with NSA so long as the Clipper technology was made available on a timely basis. On the same day in April that the President proclaimed the Clipper Initiative, "AT&T announced it would use the new chip in all its secure non-government telephones."[6]

But the chips that implement Clipper have been delayed through manufacturing difficulties. So in early August AT&T announced immediate availability of two new non-Clipper, non-key escrow telephone security devices, using AT&T proprietary algorithms, one approved for export, the other not. At the same time, Cylink, a manufacturer of security equipment, announced a DES-based phone security device.

It would seem that in a little less than a year, we have come full circle. Once again there are telephone security devices (DES and non-DES) on the market, this time in open competition with the Government's proposed key escrow system that was intended to replace an earlier DES-based offering.

3. <u>What are the Real Issues with Key Escrow</u>

What impact will these new products have on the Government's voluntary program to have key escrow systems become widely used? Will the law abiding public prefer to buy secure

---

[3] AT&T Telephone Security Device brochures presented to the Congressionally chartered CSSPAB in September, 1992.

[4] Testimony by Dr. Clinton Brooks on June 2, 1993, before the CSSPAB.

[5] The Government has chosen to call the process of storing keys for access by law enforcement authorities "key escrow." The term "escrow" has specific legal meaning, and its use here implies a legal formalism beyond what appears to be provided. The draft Escrow Encryption Standard cites a definition of escrow as having delivered something "to a third person to be given to the grantee only upon fulfillment of a condition." As pointed out by Janlori Goldman, both the "escrow agents," who will hold the keys, and the law enforcement community are part of the Executive Branch of the Federal Government and can hardly be considered truly third parties in the legal sense. Rather than "key escrow," many refer to this simply as "the Government has your keys."

[6] The *Washington Post*, April 17, 1993, page 1.

phones with or without key escrow, or just not buy them at all? And where is all of this headed in the computer communications world? Do we need/want key escrow capabilities for our communications? Can we afford the price we will have to pay for them? Before we can answer these questions we need to examine a number of difficult issues from practical, economic, and philosophical perspectives.

Law Enforcement's Wiretap Capabilities

An analysis of the prospects for the law enforcement community being able to maintain its present level of wiretap capability is contained in Appendix A. Through examination of a series of scenarios ranging from doing nothing to mandatory enforcement of key escrow cryptography for all phones in the U.S., it becomes clear that irreversible advances in digital telephony technology and growing availability of encryption will make it increasingly difficult to wiretap the communications of sophisticated criminal elements, with or without key escrow capabilities.

Conclusion:

With respect to the feasibility of law enforcement's being able to continue present day telephone wiretaps of illegal activities:

- Over the next few years, the law enforcement community will probably lose the technical ability to wiretap sophisticated criminal activities, regardless of whether we install key escrow systems or not, and conversely,

- the law enforcement community will almost certainly retain the technical ability to wiretap law abiding citizens and unsophisticated criminals, regardless of whether we install key escrow systems or not.

Key Escrow Applied to Telephones and Computer Communications

The limited available information concerning how key escrow techniques will work for telephone and computer communications systems is analyzed in Appendix B. Key escrow techniques appear relatively straight forward in simple point-to-point telephone situations, but their application to sophisticated computer communications environments is much more complex. While technically feasible, these applications will be subject to a wide variety of software bypasses of the hardware-only key escrow provisions that will defeat their effectiveness. They will also impose a unique hardware expense on the user which will be unacceptable in most situations.

Conclusion:

With respect to the use of key escrow for telephone communications:

- The emergence of the non-key escrow telephone security devices (such as the new AT&T and Cylink devices) will confuse the market place and deprive the Government of its hoped for widespread voluntary use of key escrow.

With respect to the use of key escrow for computer network communications:

- Significant technical and legal complications confront the use of key escrow in computer applications. The Government's hardware-only restrictions for key escrow systems cannot be achieved in computer systems where software controls the basic applications for file transfer, electronic mail, and electronic commerce. No specific requirement for law enforcement wiretap of computer communications has been identified. Conventional search warrant procedures may be adequate for obtaining computer data rather than key escrowed wiretaps.

International Acceptance of Key Escrow

The issues of international acceptance and use of key escrow techniques seem to have been poorly thought out in the Clipper plan. The sharing of escrowed keys with other governments opens technological, political, and psychological issues that are likely to be insurmountable. One need only consider the feelings of a U.S. citizen whose encryption keys were available to a collection of foreign interests to recognize that foreign interests will feel the same way about U.S. Government key escrow. While one can understand how individual governments might see advantages in such sharing, it is difficult to see how individual citizens anywhere will find the use of key escrow acceptable. In a world of growing multinational economies, key escrow arrangements among individual governments seem sadly out of place.

The Skipjack[7] Algorithm and Key Escrow Control Procedures

The Government's Skipjack review team found[8] that the algorithm used in the Clipper chip is

[7] Skipjack is the name for the encryption algorithm used in the Clipper Chip.

[8] "SKIPJACK Review Interim Report: The SKIPJACK Algorithm," July 28, 1993, by Ernest Brickell, Dorothy Denning, Stephen Kent, David Maher, and Walter Tuchman.

sound and not subject to easy defeat by exhaustive key search[9] or shortcut attacks. I am fully prepared to accept this team's findings both because of the quality of people who performed the analysis and the belief that NSA would not introduce a flaw in an algorithm of this type. But the problem with Clipper, if there is one, will not be in the algorithm itself but with the key escrow control procedures which the Government is developing to grant law enforcement access to the Clipper keys.

The key escrow control procedures, which are still not fully worked out, are intended to provide law enforcement with rapid access to keys while protecting the public from improper disclosure to unauthorized individuals. As described to the CSSPAB on July 29, 1993, the procedures appear to provide very limited protection against a government official who might be operating in an illegal manner.

Constitutional Rights Issues

Many people have discussed concerns about possible violations of the Constitutional rights of individual citizens by the use of key escrow procedures. I will defer such questions to others with a legal background.

I do have one concern regarding the comment in the President's April 16 announcement that "the Administration is committed to policies that protect all Americans' right to privacy while also protecting them from those who break the law." These two goals seem impossible to achieve at the same time. This seems to be more a "right to privacy from everyone but the Government," which is a long way from the Bill of Rights.

Overall Conclusion:

> Key escrow technology will NEITHER advance the public's right to privacy NOR protect it "from those who break the law."

As desirable as those goals may be to the Government, the technical, economic, and personal privacy aspects of key escrow techniques will limit them from playing a significant role in our future telephone and computer communications systems.

As our communication technologies continue their rapid evolution, we must be careful not to hamstring them with restrictive "solutions" to issues that have been overtaken by technology.

---

[9] The Skipjack team cites several exhaustive key search attacks on the Skipjack 80-bit key space that are useful when compared with the present U.S. Government approved-for-export 40-bit key size. They postulate a $50M machine consisting of 100,000 processors that takes 4 million years to exhaust an 80-bit key space. Such a machine could check a 40-bit key space in 8.15 hours. They also speculate on a $1.2B machine with a 1GHz clock speed that takes 1 year to search an 80-bit key space. A machine 10,000 times slower or with 1/10,000 the processors could check a 40-bit key space in just over 1 second. An 80-bit key space is very strong and a 40-bit key space is extremely weak!

4. But what about protecting "all Americans' right to privacy"?

Even if key escrow can't assure the protection of Americans "from those who break the law," we can make progress on the other theme of the Clipper announcement, the protection of "all Americans' right to privacy"!

There are several issues to be considered here:

- Good cryptography (of the quality of DES) is already available worldwide and attempts to contain it in the U.S. are only hurting U.S. users and vendors.

- Because of export restrictions, U.S. manufacturers are reluctant to integrate good cryptography into their products since they cannot sell them to the majority of their markets. This has multiple negative effects, such as:

  - denying U.S. users good quality integrated encryption products even for use only in the U.S.,

  - denying U.S. computer vendors significant overseas sales which automatically go to foreign vendors, and thus,

  - exporting U.S. jobs in computer related industries to foreign countries.

An ongoing study of foreign availability of cryptography[10] has in only a few weeks found several hundred products, most of them DES-based, that are available just about anywhere in the world. Many of these products, being sold in the U.S., are from foreign manufacturers since many countries' export laws, while claiming to be similar to those of the U.S., make it quite easy to get export licenses to the U.S. Several German DES products are routinely sold here through a blanket export license. But once here, those products cannot leave the U.S. This situation effectively guarantees that whatever worldwide business there will be in products that use cryptography will go to those companies in those countries that can readily export their products. The U.S. is losing this very important and rapidly growing market.

And it's not just the sale of products that use cryptography that we are losing. When U.S. companies cannot supply reasonable cryptography fully integrated into their entire product line, they are losing the sale of major information systems, of which the cryptographic products may be only a small portion.

Mass market software is one of the few industries where the U.S. holds a significant technological and commercial advantage. Yet U.S. producers are reluctant to incorporate cryptography into their products, solely because of U.S. export uncertainty. The Software

---

[10] Sponsored by the Software Publishers Association, prompted in part by U.S. Government officials' insistence that they were unaware of the availability of foreign cryptographic products.

Publishers Association, in a major shift in U.S. export policy in 1992, obtained blanket export permission for encryption products using keys limited to 40-bit key lengths. However, the world market, which already has ready access to 56-bit key DES products, recognizes the weakness of 40-bit keys and simply will not accept them.

Government officials[11] complain that industry cannot provide an economic analysis of how much business is being lost through the imposition of export controls on cryptography. They have a right to complain, but they must understand that this is a rapidly emerging economic environment. Once we can document in detail what we are losing or have lost, the situation will be so far along that we will be out of the game and unable to recover. We must look at the indicators and adjust our strategy based on them or we will lose much more than the sale of a few cryptographic devices.

DES is not in the public domain?

The U.S. Department of State has declared that information about cryptography that is not in the public domain cannot be exported. When faced with the question, "Isn't DES in the public domain?" they insist that it is not. To do otherwise, of course, would be to admit that DES could be readily exported, which they are determined not to allow. If exportability of good quality encryption products were not a critical issue for the U.S. computer industry, this U.S. Government policy would be just one more case where policy ignores reality. Unfortunately, it's much more important than that!

All of the information needed to implement DES has been widely published as a U.S. Government Standard[12] for 17 years. In 1986, the International Standards Organization (ISO) approved DES as an international standard, DEA-1. Later, the ISO decided it should not standardize on any cryptographic algorithm, and DEA-1 was not published as an ISO standard. Even so, DES is probably the most widely known and accepted encryption algorithm in the international community. Books and articles are routinely published telling how to implement DES in software and indeed giving the code to do it. Products that use DES in software and hardware are routinely available worldwide. How long must our Government harm the American people with policies that have no basis in reality?

Conclusion:

With respect to the impact of export controls on U.S. commercial interests, the present Government policies on export of cryptography are:

- Depriving U.S. businesses of the ability to protect their sensitive information in a routine and economic manner,

---

[11] Dr. Ray Kammer, Deputy Director of NIST on July 30, 1993, at the CSSPAB hearing.

[12] Federal Information Processing Standard (FIPS) Publication Number 46.

- Depriving U.S. computer businesses of a rapidly growing worldwide market in information products that contain a reasonable degree of security protection,

- Encouraging the development of such products outside the U.S., and

- Exporting U.S. jobs to overseas manufacturers.

Why does the Government insist on export controls?

Presumably, the reason for the Government's strangle hold on export of cryptography is to prevent its widespread use against law enforcement and other legitimate government interests.

But the issue is not simply law enforcement's desire to continue to wiretap criminals' phones. The not-so-invisible force behind all of this is the national security interest to intercept traffic from foreign sources for intelligence purposes. Somehow this is the deep dark secret that everyone knows but no one is supposed to mention.

The conflict of interest referred to in the President's Clipper announcement is not just law enforcement desires versus the public's need for good cryptography but these much more important national security interests versus the public's need to protect its sensitive information.

Conclusion:

With respect to law enforcement and national security interests in intercepting communications in general:

> Good quality encryption technology to protect communications from eavesdropping is becoming widely available throughout the world. This inevitable shift in technology will make it increasingly difficult for law enforcement and national security interests to intercept communications, irrespective of any technical or legal measures the U.S. Government might take to prevent it, including government export controls on encryption technology or government imposed key escrow systems.

Why is key escrow technology being proposed?

A recent Administration publication of Questions and Answers on the Initiative[13] contained the following, within the answer to this question:

---

[13] "Key Escrow Encryption Technology," from John D. Podesta, Assistant to the President and Staff Secretary for the White House, to Jerry Berman of the Digital Privacy and Security Working Group, dated July 29, 1993.

> "With growing availability of lower cost, commercial encryption technology for use by U.S. industry and private citizens, it became clear that a strategy was needed that could accommodate the needs
>
> - of the private sector for top notch communications security;
> - of U.S. industry to remain competitive in the world's secure communications market; and
> - of U.S. law enforcement to conduct lawfully authorized electronic surveillance."

From the above analysis it should be clear that:

- while Skipjack represents very strong cryptography, with key escrow added, few will view it as "top notch communications security,"
- just as with the 40-bit key "solution," key escrow will not allow "U.S. industry to remain competitive" in any international market, and
- law enforcement will find it increasingly difficult to conduct wiretaps, with or without key escrow capabilities.

In short, none of these stated goals is achievable.

The same "answer" then went on to say:

> "Enhancing the Government's ability to decrypt non-key escrow encryption used by the targets of authorized law enforcement wiretaps is another possible strategy for coping with the effects of encryption on law enforcement. However, since encryption appears in a number of forms and applications, the costs are likely to be substantial and may not be either affordable or practical given the requirement for 'real time' decryption in the course of wiretap operations."

Enhancing the ability to decrypt non-key escrow encryption may well be the only practical measure that the law enforcement and national security communities can take. As a minimum, the costs of these alternatives should be well understood before we launch into a massive key escrow process that has been demonstrated to have little likelihood of achieving its goals.

5. A National Dilemma!

This situation is truly a dilemma of national importance that can not be resolved with a "one way or the other" decision but must involve a compromise of the interests of both sides. Key escrow was a good try at a solution, but as the above analysis indicates, it will not be acceptable against the harsh realities of economics and human nature. Some form of "cryptography which is good enough for the public's use even if it may make the national security task harder" compromise must be reached.

For over fifty years, the national security side of this story has always had the interest of every U.S. Administration and for good reason. "Codebreaking is the most important form of secret intelligence in the world today. It produces much more and much more trustworthy information than spies, and this intelligence exerts great influence upon the policies of governments."[14] Breaking the codes of others has been and continues to be a vital aspect of our national security.

But we are now in an international world of interconnected communications systems carrying all kinds of sensitive information vital to our economic and national well being. Technology has advanced to the point where cryptography is both highly feasible and desirable for use by private citizens and business. It is dangerous to deny ourselves the ability to protect our own sensitive information in the hope that we may still be able to eavesdrop on others.

We must face the fact that foreign interests already have good cryptography which they will increasingly use to protect their communications no matter how the U.S. Government tries to impede them. If they do not employ good cryptographic mechanisms and practices, it is for reasons other than their unavailability.

It is essential that we hear from the other side, the interests and needs of the public to protect its information, so that we can weigh the two issues and reach a carefully considered resolution to this dilemma for today and the future.

As cryptography becomes more widespread, the ability to routinely intercept and read such traffic will inevitably get harder. Key escrow, if it were to become very widely used, could make both the law enforcement and national security community's jobs much easier.

But key escrow will not become widely used outside of government. The new non-key escrow phone devices will outsell all Clipper phones (except for the devices that the Government forces itself to buy). Key escrow will never find a significant market in the computer communications world for the simple economic reason that it will cost more then software encryption. No one who is not forced to use key escrow will choose to pay extra for it.

And, as discussed in the Appendices, attempts to mandate the use of key escrow or to outlaw other forms of encryption will not succeed even if given the force of law.

---

[14] From the Preface of *The Code-Breakers* by David Kahn.

The Final Conclusion

Key escrow is not the panacea that its inventors envisioned. It will not drive out DES and other good cryptographic systems. In a very real sense, the President's Clipper Chip Initiative has sounded the alarm for those who once viewed cryptography as solely of interest to the technicians. It may well have galvanized opposition to unreasonable and restrictive government export control policies in this area once and for all.

Just as the law enforcement community has to face the fact that no matter what we do, wiretaps are going to be less useful in the future because of advances in technology, so the intelligence community has to face the fact that it will become progressively harder to listen in to others. Over the years, the Government's policy of denying export of cryptographic devices has perhaps slowed this inevitable trend a little. But, increasingly, the negative effects of these policies on U.S. business, both on users and suppliers of these technologies, far outweigh any positive effect that further restrictions can have.

Others have and will use good quality cryptography whether we allow ourselves to do so or not. We must not penalize ourselves by further restricting cryptography, either through poorly founded export policies or poorly thought out technologies such as key escrow.

6. So where do we go from here?

The Administration is currently conducting an "Interagency Review" as called for in the President's April announcement. Input from the public is being received from the testimony at meetings such as from the CSSPAB and from groups such as the Digital Privacy and Security Working Group as well as industry and the public at large. This Interagency Review is not, however, a public debate of the issues confronting us. The interests of the commercial sector and of the public at large are not well represented here.

Recent proposed Congressional legislation[15] has called for the establishment of a "Comprehensive Independent Study of National Cryptography Policy" by the National Research Council. Such a study is welcomed as a means for exploring all sides of this most important issue even if it does put off resolution of the issue for up to two years.

In any case, it is essential that the Congress become involved in the timely resolution of this issue in a way that properly balances the law enforcement and national security interests with those of the public to protect its sensitive information.

---

[15] H.R.2401 as reported by House committee, July 30, 1993, House Report No 103-200, Item 77: (34) Sec. 262. Comprehensive Independent Study of National Cryptography Policy. This bill is scheduled for further action on Sept. 8.

APPENDIX A

What can law enforcement expect from wiretaps in the future?

The FBI and other law enforcement experts have made strong and sometimes impassioned pleas that we not let technology advances deny them the opportunity to tap into phone conversations of illegal activities. Acknowledging the relatively small number of wiretaps per year and the difficult process that the court system requires for obtaining a wiretap, they argue persuasively that the value of wiretaps in organized/white collar crime is invaluable and must not be lost.

The possibility of encountering scrambled communications that cannot be decrypted is the concern being addressed by the Government's Clipper initiative. However, there are many other concerns inherent in the digital telephony issue that were acknowledged by the FBI during the Board's hearings to be of greater concern than encryption.[1]

One of the very serious aspects of this problem involves extending wiretaps beyond the "reach" of the telephone central office. A wiretap on a home phone can be effected entirely at the telephone company central office. A wiretap on a business phone connected by a private branch exchange (PBX) cannot be directly tapped by the phone company. In earlier proposed legislation, the FBI sought technical solutions to the digital telephony problems that would ensure they would not lose their ability to wiretap illegal communications.

Few would argue that the public wants the law enforcement community to provide effective protection against all forms of criminal activity. This situation argues strongly for keeping wiretaps as effective as possible for the benefit of the law enforcement community and the public in general.

But what is the future for wiretaps, anyway?

Since key escrow procedures have been identified as the Government's fundamental means of ensuring the continuation of effective wiretaps, it is essential that we examine just how effective wiretap capabilities will be in the future, whether we establish key escrow procedures or not.

Today (prior to the recent AT&T phone security announcement), only a few relatively expensive telephone encryption capabilities are available, and very few wiretaps encounter encrypted communications.[2] Today, the general public and apparently most criminals use the

---

[1] Jim Kallstrom, FBI, in answer to a question before the CSSPAB on July 29, 1993.

[2] Jim Kallstrom, FBI, in answer to a question at a Clipper Briefing April 24, 1993, at the New Executive Office Building, Washington, DC.

public phone system to communicate without additional protection and are thus subject to conventional wiretaps.

One way to understand how things may turn out in the future is to postulate a series of scenarios and examine the different outcomes.

If we do nothing:

There are techniques available today for encrypting phones; however, because this whole topic of wiretaps and encryption has until now been of obscure interest only to technicians, the criminal element probably has not bothered to use them. Now that high- level attention is being called to this issue, one can easily conjecture that sophisticated criminals (those who understand the threats to their activities and the availability and cost of countermeasures) are actively looking for ways to protect themselves from wiretaps. In this scenario, the Government will retain the ability to tap the communications of ordinary citizens and average criminals but lose access to the communications of the sophisticated criminal.

If non-key escrow devices become widely available:

In the absence of any other actions by the Government, if non-key escrow telephone encryption devices (such as the new AT&T devices) become widely available, then the sophisticated criminal will use these devices to protect his or her communications from wiretaps. That is the stated reason[3] that NSA reacted so strongly against the original AT&T DES phone security device. Other criminal elements (the average ones) will probably keep using the phone system without protection. Thus the Government will again retain the ability to tap the phones of ordinary citizens and average criminals but lose the ability to tap the phones of sophisticated criminals.

If the Government equips every phone with key escrow:

Suppose the Government decided that the wiretap issue is of such importance that it would pay to have every phone in the country equipped with a key escrow capability so that all phone calls would be subject to easy decryption in the case of a wiretap. Most citizens and average criminals would no doubt continue to use the new key escrow phone system in the same way they use phones today, thus remaining subject to wiretaps. However, sophisticated criminals, realizing what is happening, would likely resort to other means (such as super encryption or use of the new AT&T devices) to protect their communications on top of the key escrow devices, thus exempting themselves from wiretaps. In this scenario, the Government will retain the ability to tap ordinary citizens and our average criminals but still lose access to the communications of the sophisticated criminal (if this looks repetitive, it is).

---

[3] Testimony by Dr. Clinton Brooks on June 2, 1993, before the CSSPAB.

Or, if the Government outlaws all non-key escrow encryption:

Another scenario is the often mentioned case in which the Government outlaws all forms of encryption except those that use key escrow. (Please ignore the civil liberty issues that would arise from such an action for this discussion.) Once again most citizens, including average criminals, would continue to use the phone system (mostly in the clear with only limited key escrow capability installed), the same as they do now. These people would continue to be subject to the same level of wiretap as today. But the sophisticated criminal who is undeterred by using illegal technology will have no qualms about supplementing his or her telephone security and thus will be able again to escape law enforcement's wiretap capability. Once again, the result is the same as for the preceding scenarios.

Or, ... others?

The reader is encouraged to examine other scenarios. But I postulate that all will result in the same conclusion we saw repeatedly in the above cases: in the future, for those elements who wish to protect their communications against interception by the Government or anyone else, there is nothing the Government will be able to do to stop them. Key escrow procedures will not alter this situation.

Technology evolves, whether we like it or not

The Government, like other elements of society, is subject to shifts in technology, which in some cases bring forth new and wonderful capabilities but at times also eliminate capabilities previously enjoyed.

- The laser reader at the grocery checkout allowed grocery chains to run much more efficiently but also took away individual pricing, which many people dearly miss.

- The bomber was a terrifying threat until radar allowed improvements to defensive measures. Stealth technology has now shifted that balance again to the offensive.

But we don't hear cries to ban stealth technology or to insist that the other guy put a little reflector on his Stealth planes so our radar can detect them. We accept the shift in technology for what it is and do as best we can.

The balance of technology has long favored the ability to wire tap communications. With widespread use of private branch exchanges and cryptography, that balance will shift no matter what else we might do to attempt to slow it. We must be careful in our haste to impede this technological shift lest we introduce expensive and invasive capabilities that do not achieve what we desire.

APPENDIX B

How will key escrow work?

The original Clipper announcement indicated that the Initiative was to be used for telephone-like communications, at least for now. Many in the computer industry have been concerned about the impact of a hardware-only key escrow solution on their ability to supply products employing cryptography. An examination of the information supplied to date on key escrow provides a basic understanding of how key escrow will work domestically in telephone systems but little insight into its use in computer systems, or internationally.

On July 30, 1993, NIST unveiled a draft "Escrowed Encryption Standard" that describes, often in purposefully vague terms, how a key escrow system will work. It includes a statement of applicability for voice, fax, and data limited communication levels of up to 14.2 Kbps and below. (For those not into communications jargon, that amounts to voice-grade, point-to-point communication links such as when one picks up the phone to dial another person or send a fax.) The application of key escrow to high bandwidth computer communications networks is apparently being left for later documents.

The Government has insisted that the encryption being used for key escrow must be kept secret and only made available in hardware versions that are highly tamper resistant so that the key escrow measures cannot be subverted or bypassed.

First for telephones ...

The operation of telephone security devices (such as the AT&T 3600 "bump-in-the-wire"), in the absence of key escrow, can readily be understood. In such devices, the user (typically a person rather than a computer) places a phone call and, once a connection has been established with the desired parties, presses the "secure" button which initiates the synchronization of both parties' encryption devices. At this point encrypted communication proceeds until either party hangs up or presses the "clear" button. This is approximately how the original AT&T 3600 that uses the DES operates.

The addition of key escrow to such a device occurs approximately as follows. After the "secure" key is pressed and the cryptographic synchronization has taken place, each device generates a special "Law Enforcement Access Field" (LEAF) and exchanges it with the device at the other end of the connection. The LEAF contains, among other things, an encrypted version of the device's unique identification number.

If a wiretap is in place when the "secure" key is pressed, the wiretap authorities will be able to detect the LEAF and extract the unique id, which can then be sent to the Government key escrow agents (two of them are envisioned at present for added protection from improper use). Each key escrow agent will return his/her instance of the device's unique key in encrypted forms that together will allow the wiretap authority to decrypt the scrambled communications.

The equipment that the wiretap authority will need to detect key escrowed telephone communications and ascertain the target device's unique id will be relatively straight forward. Once it detects the synchronization exchange between encryption devices, it need only wait until the LEAF is sent to pick up the device's ID.

How will the exchange with the key escrow agents take place?

How the actual exchange between the law enforcement authority and the two key escrow agents will occur has not been publicly stated (at least as of this writing[1]). The escrow agent must determine that the law enforcement authority has a valid wiretap court order even though he or she must not be told whom the wiretap is for or to whom the device ID belongs. The exchange between the wiretapper and the two key escrow agents must happen quickly because real-time taps of urgent phone calls may be taking place.

Under these circumstances, it is difficult to comprehend what particularly critical role the escrow agent is performing since he or she has virtually no information on which to base a decision to send the device's unique key to the wiretapper. It is also difficult to see how the audit trail that each escrow agent must keep will be of any value in detecting misuse of the system since all it contains is the fact that a requested key was returned to a particular wiretap authority at a particular time.

How many intercept devices there will be has not yet been determined. One per law enforcement jurisdiction seems too many, one per locality having wiretaps last year doesn't seem right, and a few stockpiled in Washington with the key escrow agents feels wrong.

And who will pay for all of this?

How much the key escrow service will cost and who will pay for it have not yet been determined either. Presumably, the Government will pay for the costs of acquiring, storing, cataloging, and accessing escrow keys, though it may seek an increase in the Federal excise tax on phone use to fund it. The user will have to pay for the device (unless the scenario in which the Government pays for everything comes about). The price of the AT&T devices today is approximately $1200 each. Presumably, the Clipper version of the AT&T device will not cost the consumer any more (even though because of the extra Clipper chip it will cost AT&T more to make). But unless the Clipper version is actually lower in price than the non-key escrow devices, it is difficult to see why a consumer will choose the key escrow

[1] The information in this section of the paper is derived from the testimony of Mr. Geoffrey Greiveldinger, Special Counsel, Narcotic and Dangerous Drug Section of the Department of Justice before the CSSPAB on July 29, 1993.

version over the ordinary one. It also remains to be seen how many people are willing to pay extra (even if the price drops by a factor of ten) for any form of telephone security.

<u>... and then for computer communications?</u>

Typically, computer-to-computer communications such as electronic mail do not involve a time synchronization between the sender and the receiver. One can originate mail that takes minutes or hours to deliver, and the receiver can take days to get around to reading it. So the equivalent of one user pressing the "secure" button to synchronize the encryption devices with the receiver does not exist.

Today's electronic mail security services typically use a pseudo random number to encrypt the text of the message to be sent and then encrypt that message key using the receiver's public key to protect it during transmission and send it along with the encrypted message. The receiver's process looks up his or her private key, decrypts the message key, and then decrypts the message itself. It would be possible to have the originating process generate a LEAF and send it along with the message so that any wiretap could identify the unique ID of the sender. This would, of course, require a LEAF for every message sent.

Is hardware-only encryption feasible?

The Government has stated a firm requirement that the encryption process must be performed in hardware to protect the integrity of the encryption itself and the resulting LEAF. Clearly that portion of the system that does the encryption can be implemented in a hardware device or smart card or PCMCIA card. The electronic mail (or other) application system itself will at some level be implemented in software on a host computer, personal computer, or workstation. That software, while it probably cannot compromise the hardware, can certainly bypass it, leaving out or modifying the LEAF. Such action could result in unsuccessful decryption by the receiver's hardware device.

But there are several scenarios in which groups of people who want to defeat the key escrow process will certainly be able to do so. The first case involves using another software encryption process (such as Pretty Good Privacy [PGP] or Privacy Enhanced Mail [PEM]) to superencrypt the message before sending it to the key escrow encryption hardware. The message would have a legitimate LEAF and be fully compliant with the latest version of the Escrowed Encryption Standard. But if the law enforcement authorities ever try to decrypt it, they will find the superencrypted message underneath.

A second approach at defeating the escrow process would be for the software that processes the message after it has been encrypted by the key escrow hardware to save the LEAF and modify the one that is contained in the message so that it looks okay. The real LEAF could be forwarded in parts in other portions of the communications protocols so that the receiving system could reconstruct the proper LEAF, reinsert it in the message, and send the message to the key escrow decryption hardware. Any law enforcement use would, of course, be thwarted by the improper LEAF.

A third approach would be to just encrypt the message after it has been through the key escrow hardware so that the message, LEAF and all, would be encrypted. Of course, if one is going to do this, one would not bother with the key escrow hardware in the first place.

The point of all this is that truly hardware-only implementations of key escrow techniques are not possible in computer applications. Within a very short time after the introduction of key escrow systems, software patches for most popular application programs to defeat key escrow without detection (until a wiretap is attempted) will be available on free software bulletin boards everywhere. Anyone who wants to protect their communications from wiretap can do so easily without detection. Even if the Government were to mandate the use of key escrow hardware, one can quickly expect software implementations that look like the hardware output (but won't work on a wiretap) to crop up just to save the extra cost of purchasing the hardware.

Interception complexity

The problems for the interceptor are considerably more difficult than in the telephone case. First of all, the wiretap must capture all of the data being sent to be effective. This will be okay if the direct link to the user's computer is tapped, but much more difficult if only one of the many links in the wide area network over which the user's data is sent can be tapped, since only portions of the communications may be intercepted.

The interceptor's device must understand all of the computer protocols up to and including the specific electronic mail or other application protocol to be able to find the LEAF in the maze of protocol layers. Given today's sophisticated protocol handling devices, building such an interception tool is not considered a technological challenge, but a general purpose tool capable of intercepting LEAFs in a wide variety of application layer protocol streams will be considerably more complex than the simple telephone interception device.

Legal side of broad network wiretaps?

It is also worthy of some legal scholar's review to determine if the provisions in the wiretap statute that require minimization of the intercept of traffic other than that associated with the actual wiretap target will render blanket searches of wide area network links illegal. It certainly will be hard to avoid examining massive quantities of information that have absolutely nothing to do with the wiretap target in such a search.

All of these concerns taken together make it clear that implementing key escrow encryption in the large number of existing and future applications for computer communications will be a much more difficult task than that envisioned for telephone systems.

And who will pay?

Once again, presumably the Government will pay for the interception costs, but the user will have to pay for the actual hardware devices that are employed. The cost of $25 per chip translates into $100 per device, once it is packaged and documented for end user installation. If one envisions 10 million such devices put into operation in the next few years, that amounts to $1 billion in extra cost to the user community. This cost must be weighed against the essentially free software packages that are available. And for what capability?

<u>But does the FBI really need to obtain computer traffic by wiretap?</u>

In all the comments I have seen to date, no one has indicated that the law enforcement community needs wiretaps to obtain computer communications. Most computer systems have automatic backup capabilities that keep archive copies of all files in case of equipment failures. Law enforcement authorities can obtain copies of electronic mail or other computer files through traditional search warrant procedures instead of resorting to difficult-to-obtain wiretaps. A counter argument might be that searches yield historical data while wiretaps yield real-time data. But until there is a demonstrated need for a capability, we must not use the possibility that we might want something as the excuse to pursue a path that is contrary to technological evolution.