

Department of Commerce
National Institute of Standards and Technology
Computer System Security and Privacy Advisory Board

Review of Cryptography Policy
June 1993

Statement of CPSR Washington office
Marc Rotenberg, director
(rotenberg@washofc.cpsr.org)
with David Sobel, legal counsel,
Dave Banisar, policy analyst

Mr. Chairman, members of the Advisory Panel, thank you for the opportunity to speak today about emerging issues on cryptography policy.

My name is Marc Rotenberg and I am director of the CPSR Washington office. Although CPSR does not represent any computer firm or industry trade association, we speak for many in the computer profession who value privacy and are concerned about the government's Clipper proposal.

During the last several years CPSR has organized several meetings to promote public discussion of cryptography issues. We have also obtained important government documents through the Freedom of Information Act. We believe that good policies will only result if the public, the profession, and the policy makers are fully informed about the significance of these recent proposals.

We are pleased that the Advisory Board has organized hearings. This review of cryptography policy will help determine if the Clipper proposal is in the best interests of the country. We believe that a careful review of the relevant laws and policies show that the key escrow arrangement is at odds with the public interest, and that therefore the Clipper proposal should not go forward.

Today I will address issues 1 through 3 identified in the NIST announcement, specifically the policy requirements of the Computer Security Act, the legal issues surrounding

the key escrow arrangement, and the importance of privacy for network development.

1. CRYPTOGRAPHY POLICY

The first issue concerns the 1987 statute enacted to improve computer security in the federal government, to clarify the responsibilities of NIST and NSA, and to ensure that technical standards would serve civilian and commercial needs. The Computer Security Act, which also established this Advisory Panel, is the true cornerstone of cryptography policy in the United States. That law made clear that in the area of unclassified computing systems, the Department of Commerce and not the Department of Defense, would be responsible for the development of technical standards. It emphasized public accountability and stressed open decision-making.

The Computer Security Act grew out of a concern that classified standards and secret meetings would not serve the interests of the general public. As the practical applications for cryptography have moved from the military and intelligence arenas to the commercial sphere, this point has become clear. There is also clearly a conflict of interest when an agency tasked with signal interception is also given authority to develop standards for network security.

In the spirit of the Computer Security Act, NIST set out in 1989 to develop a public key standard FIPS. In a memo dated May 5, 1989 and obtained by CPSR through the Freedom of Information Act, NIST said that it planned:

to develop the necessary public-key based security standards. We require a public-key algorithm for calculating digital signatures and we also require a public-key algorithm for distributing secret keys.

NIST then went on to define the requirements of the standard:

The algorithms that we use must be public, unclassified, implementable in both hardware or software, usable by federal Agencies and U.S. based multi-national corporation, and must provide a

level of security sufficient for the protection of unclassified, sensitive information and commercial propriety and/or valuable information.

The Clipper proposal and the full-blown Capstone configuration, which incorporates the key management function NIST set out to develop in 1989, is very different from the one originally conceived by NIST.

- The Clipper algorithm, Skipjack, is classified,
- Public access to the reasons underlying the proposal is restricted,
- Skipjack can be implemented only in tamper-proof hardware,
- It is unlikely to be used by multi-national corporations, and
- Its security remains unproven.

The Clipper proposal undermines the central purpose of the Computer Security Act. Although intended for broad use in commercial networks, it was not developed at the request of either U.S. business or the general public. It does not reflect public goals. Rather it reflects the interests of one secret agency with the authority to conduct foreign signal intelligence and another government agency responsible for law enforcement investigations.

It is our belief that the Clipper proposal clearly violates the intent of the Computer Security Act of 1987. What is the significance of this? It is conceivable that an expert panel of cryptographers will review the Skipjack algorithm and find that it lives up its billing, that there is no "trap door" and no easy way to reverse-engineer. In fact, the White House has proposed just such a review process

But is this process adequate? Is this the procedure the Advisory Board would endorse for the development of widespread technical standards? The expert participants will probably not be permitted to publish their assessments of the proposal in scientific journals, further review of the standard will be restricted, and those who are skeptical will remain in the dark about the actual design of the chip. This

may be an appropriate process for certain military systems, but it is clearly inappropriate for a technical standard that the government believes should be widely incorporated into the communications infrastructure.

Good government policy requires that certain process goals be satisfied. Decisions should be made in the open. The interests of the participating agencies should be clear. Agencies should be accountable for their actions and recommendations. Black boxes and government oversight are not compatible.

There is an even greater obligation to promote open decisions where technical and scientific issues are at stake. Innovation depends on openness. The scientific method depends on the ability of researchers to "kick the tires" and "test drive" the product. And, then, even if it is a fairly good design, additional testing encourages the development of new features, improved performance and reduced cost. Government secrecy is incompatible with such a development process.

Many of these principles are incorporated into the Computer Security Act and the Freedom of Information Act. The current government policy on the development of unclassified technical standards, as set out in the Computer Security Act, is a very good policy. It emphasizes public applications, stresses open review, and ensures public accountability. It is not the policy that is flawed. It is the Clipper proposal.

To accept the Clipper proposal would be to endorse a process that ran contrary to the law, that discourages innovation, and that undermines openness.

2. LEGAL AND CONSTITUTIONAL ISSUES

There are several legal and constitutional issues raised by the government's key escrow proposal.

The premise of the Clipper key escrow arrangement is that the government must have the ability to intercept electronic communications, regardless of the economic or societal costs. The FBI's Digital Telephony proposal, and

the earlier Senate bill 266, was based on the same assumption.

There are a number of arguments made in defense of this position: that privacy rights and law enforcement needs must be balanced, or that the government will be unable to conduct criminal investigations without this capability.

Regardless of how one views these various claims, there is one point about the law that should be made very clear: currently there is no legal basis -- in statute, the Constitution or anywhere else -- that supports the premise which underlies the Clipper proposal. As the law currently stands, surveillance is not a design goal. General Motors would have a stronger legal basis for building cars that could not go faster than 65 miles per hour than AT&T does in marketing a commercial telephone that has a built-in wiretap capability. In law there is simply nothing about the use of a telephone that is inherently illegal or suspect.

The federal wiretap statute says only that communication service providers must assist law enforcement in the execution of a lawful warrant. It does not say that anyone is obligated to design systems to facilitate future wire surveillance. That distinction is the difference between countries that restrict wire surveillance to narrow circumstances defined in law and those that treat all users of the telephone network as potential criminals. U.S. law takes the first approach. Countries such as the former East Germany took the second approach. The use of the phone system by citizens was considered inherently suspect and for that reason more than 10,000 people were employed by the East German government to listen in on telephone calls.

It is precisely because the wiretap statute does not contain the obligation to incorporate surveillance capability -- the design premise of the Clipper proposal -- that the Federal Bureau of Investigation introduced the Digital Telephony legislation. But that legislation has not moved forward on Capitol Hill and the law has remained unchanged. The Clipper proposal attempts to accomplish through the standard-setting and procurement process what the Congress has been unwilling to do through the legislative process.

On legal grounds, adopting the Clipper would be a mistake. There is an important policy goal underlying the

wiretap law. The Fourth Amendment and the federal wiretap statute do not so much balance competing interests as they erect barriers against government excess and define the proper scope of criminal investigation. The purpose of the federal wiretap law is to restrict the government, it is not to coerce the public.

Therefore, if the government endorses the Clipper proposal, it will undermine the basic philosophy of the federal wiretap law and the fundamental values embodied in the Constitution. It will establish a technical mechanism for signal interception based on a premise that has no legal foundation. I am not speaking rhetorically about "Big Brother." My point is simply that the assumption underlying the Clipper proposal is more compatible with the practice of telephone surveillance in the former East Germany than it is with the narrowly limited circumstances that wire surveillance has been allowed in the United States.

There are a number of other legal issues that have not been adequately considered by the proponents of the key escrow arrangement that the Advisory Board should examine. First, not all lawful wiretaps follow a normal warrant process. It is critical that the proponents of Clipper make very clear how emergency wiretaps will be conducted before the proposal goes forward. Second, there may be civil liability issues for the escrow agents if there is abuse or compromise of the keys. Escrow agents may be liable for any harm that results. Third, there is a Fifth Amendment dimension to the proposed escrow key arrangement if a network user is compelled to disclose his or her key to the government in order to access a communications network. Each one of these issues should be examined.

There is also one legislative change that we would like the Advisory Board to consider. During our FOIA litigation, the NSA cited a 1951 law to withhold certain documents that were critical to understand the development of the Digital Signature Standard. The law, passed grants the government the right restrict the disclosure of any classified information pertaining to cryptography. While the government may properly withhold classified information in FOIA cases, the practical impact of this particular provision is to provide another means to insulate cryptographic policy from public review.

Given the importance of public review of cryptography policy, the requirement of the Computer Security Act, and the Advisory Board's own commitment to an open, public process, we ask the Advisory Board to recommend to the President and to the Congress that section 798 be repealed or substantially revised to reflect current circumstances.

This is the one area of national cryptography policy where we believe a change is necessary.

3. INDIVIDUAL PRIVACY

Communications privacy remains a critical test for network development. Networks that do not provide a high degree of privacy are clearly less useful to network users. Given the choice between a cryptography product without a key escrow and one with a key escrow, it would be difficult to find a user who would prefer the key escrow requirement. If this proposal does go forward, it will not be because network users or commercial service providers favored it.

Many governments are now facing questions about restrictions on cryptography similar to the question now being raised in this country. It is clear that governments may choose to favor the interests of consumers and businesses over law enforcement. Less than a month ago, the government of Australia over-rode the objections of law enforcement and intelligence agencies and allowed the Australian telephone companies to go forward with new digital mobile phone networks, GSM, using the A5 robust algorithm. Other countries will soon face similar decisions. We hope that they will follow a similar path

To briefly summarize, the problem here is not the existing law on computer security or policies on cryptography and wire surveillance. The Computer Security Act stresses public standards, open review, and commercial applications. The federal wiretap statute is one of the best privacy laws in the world. With the exception of one provision in the criminal code left over from the Cold War, our current cryptography policy is very good. It reflects many of the values -- individual liberty, openness, government accountability -- that are crucial for democratic societies to function.

The problem is the Clipper proposal. It is an end-run around policies intended to restrict government surveillance and to ensure agency accountability. It is an effort to put in place a technical configuration that is at odds with the federal wiretap law and the protection of individual privacy. It is for these reasons that we ask the Advisory Board to recommend to the Secretary of Commerce, the White House, and the Congress that the current Clipper proposal not go forward.

I thank you for the opportunity to speak with you about these issues. I wish to invite the members of the Advisory Committee to the third annual CPSR Privacy and Cryptography conference that will be held Monday, June 7 in Washington, DC at the Carnegie Endowment for International Peace. That meeting will provide an opportunity for further discussion about cryptography policy.

ATTACHMENTS

"TWG Issue Number: NIST - May 5, 1989," document obtained by CPSR as a result of litigation under the Freedom of Information Act.

"U.S. as Big Brother of Computer Age," The New York Times, May 6, 1993, at D1.

"Keeping Fewer Secrets," Issues in Science and Technology, vol. IX, no. 1 (Fall 1992)

"The Only Locksmith in Town," The Index on Censorship (January 1990)

[The republication of these articles for the non-commercial purpose of informing the government about public policy is protected by section 107 of the Copyright Act of 1976]

The Clipper Proposal

National Institute of Standards and Technology,
Computer System Security and Privacy
Advisory Board,
June 2, 1993

Marc Rotenberg,
CPSR Washington Office
rotenberg@washofc.cpsr.org

CPSR 1993

Clipper Premise

CP:

Telecommunications
equipment should be
designed to facilitate
surveillance

CPSR 1993

CP "Implementation"

- "S. 266" (Senate resolution on obligation to provide plaintext of communication)
- Digital Telephony Proposal (Legislative proposal to require that intercept capability be designed into communications equipment)
- Clipper Chip (Proposed government technical standard for cryptography based on key escrow)

CPSR 1993

CP Evaluation

Technical analysis of CP

- Will proposal achieve stated goal?
- Is it an efficient solution?
- What are possible risks?

Legal and policy analysis of CP

- What does the law say about the proposal?
- What is the reason for the policy?
- Is it a good policy?

CPSR 1993

Fourth Amendment and CP

The Fourth Amendment (1791)

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized."

CPSR 1993

Fourth Amendment and Electronic Communications

Supreme Court cases

Olmstead v. United States (1928) (Does Fourth Amendment apply to electronic communications?)

Katz v. United States (1967) (Established privacy of telephone communications)

Berger v. New York (1967) (Ruled state law permitting wire surveillance unconstitutional)

CPSR 1993

Passage of 1968 Wiretap law

"Privacy of communications is a basic concept in our business. We believe the public has an inherent right to feel that they can use the telephone with confidence, just as they talk face to face. Any undermining of this confidence could seriously impair the usefulness and value of telephone communications."

- Vice President, American Telephone & Telegraph (1967)

CPSR 1993

Wiretap Law and CP

1968 Federal Wiretap Statute:
Restrictions on government conduct

1. Probable cause
2. Particularity
3. Normal investigative procedures have failed or are likely to fail
4. Method of intercept specified
5. Minimization

CPSR 1993

Wiretap in Practice

- Use of wiretap by law enforcement (1992)
- Very small (VS) number of lawful wiretaps in the US (10^3 against 10^{12} calls)
- Wiretap is VS percentage of all arrests (10^3 against 10^7)
- Primarily for narcotics offenses

CPSR 1993

Wiretap Trends, 1968-1990

- Cost of wire surveillance has increased
- Number of conversations intercepted has increased
- Number of non-incriminating conversations intercepted has increased
- Number of incriminating conversations intercepted has remained unchanged
- Arrest level has remained unchanged

Source: David Banisar, CPSR

CPSR 1993

Conclusion

- No legal or policy basis for CP
- Wire surveillance is VS part of law enforcement. Effectiveness is unclear.
- Fourth Amendment and wiretap law restrict the government, they do not coerce the public
- A good policy; reflects social and legal policy goals aimed to protect privacy, restrict the government, limit abuse

CPSR 1993

EDWARD J. MARKEY, MASSACHUSETTS, CHAIRMAN

W.J. "BILLY" TAUZIN, LOUISIANA
 RICK BOUCHER, VIRGINIA
 THOMAS J. MANTON, NEW YORK
 RICHARD H. LEBMAN, CALIFORNIA
 LYNN SCHENK, CALIFORNIA
 MARJORIE MARGOLIES-MEZYNSKY,
 PENNSYLVANIA
 MIKE SYNAR, OKLAHOMA
 RON WYDEN, OREGON
 RALPH M. HALL, TEXAS
 BILL RICHARDSON, NEW MEXICO
 JIM SLATTERY, KANSAS
 JOHN BARTYNT, TEXAS
 JIM COOPER, TENNESSEE
 JOHN D. DINGELL, MICHIGAN
 (EX OFFICIO)

JACK FIELDS, TEXAS
 THOMAS J. BULLEY, JR., VIRGINIA
 MICHAEL G. OXLEY, OHIO
 DAN SCHAEFER, COLORADO
 JOE BARTON, TEXAS
 ALEX MCNILLAN, NORTH CAROLINA
 J. DENNIS HASTERT, ILLINOIS
 PAUL E. GALLAGHER, OHIO
 CARLOS J. MOOREHEAD,
 CALIFORNIA (EX OFFICIO)

U.S. House of Representatives

Committee on Energy and Commerce

SUBCOMMITTEE ON TELECOMMUNICATIONS AND FINANCE

Washington, DC 20515-6119

ROOM H2-318
 FORD HOUSE OFFICE BUILDING
 PHONE (202) 226-3424

DAVID H. MOULTON
 CHIEF COUNSEL AND STAFF DIRECTOR

April 19, 1993

The Honorable Ronald H. Brown
 Secretary
 Department of Commerce
 14th and Pennsylvania Avenue, N.W.
 Washington, D.C. 20236

Dear Secretary Brown:

As you know, I have long been interested in the privacy and security of telecommunications transmissions and data in a networked environment. Recent reports concerning the Administration's endorsement of an electronic encryption standard, based upon "clipper chip" technology, have raised a number of related issues. The international competitiveness of U.S. high tech manufacturers and the software industry is a key factor that the government should consider when addressing issues of encryption and data security. As the nation moves forward in developing the national communications and information infrastructure, security of telecommunications transmissions and network data will be an increasingly important factor for protecting the privacy of users.

The "hacker" community can compromise the integrity of telecommunications transmissions and databases linked by the network. The people and businesses that use the nation's telecommunications network and the personal computers linked through it increasingly are demanding that information be protected against unauthorized access, alteration, and theft.

I am concerned that the Administration's plan may mean that to remain competitive internationally, U.S. companies would be compelled to develop two products -- one for U.S. government customers, and another for private, commercial users who may want a higher encryption standard. This may inadvertently increase costs to those U.S. companies hoping to serve both markets. To assist the Subcommittee's analysis of this issue, please respond to the following questions:

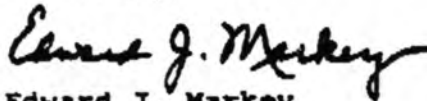
1. Has the encryption algorithm or standard endorsed by the Administration been tested by any entity other than NSA, NIST or the vendor? If so, please identify such entities and the nature of testing performed. If not, please describe any plans to have the algorithm tested by outside experts and how such experts will be chosen.

The Honorable Ronald H. Brown
Page 2
April 19, 1993

2. Under the Administration's plan, what entities will be the holders of the "keys" to decrypt scrambled data? What procedures or criteria will the Administration utilize to designate such key holders?
3. Does the encryption algorithm endorsed by the Administration contain a "trap door" or "back door," which could allow an agency or entity of the Federal government to crack the code?
4. It is clear that over time, changes in technologies used for communications will require new techniques and additional equipment. How will encryption devices adapt to the rapid advancement of telecommunications technology?
5. What additional costs would the proposed encryption place on the Federal government? What is the estimated cost to consumers and businesses which opt for the federal standard in their equipment?
6. What is the Commerce Department's assessment of the competitive impact of the Administration's endorsement of the "clipper chip" technology on U.S. exports of computer and telecommunications hardware and software products?

I would appreciate your response by no later than close-of-business, Wednesday, April 28, 1993. If you have any questions, please have your staff contact Colin Crowell or Karen Colannino of the Subcommittee staff at (202) 226-2424.

Sincerely,



Edward J. Markey
Chairman

Addison Fischer
Fischer International Systems Corporation
June 2, 1993

We enclose commentary pursuant to F.R. Doc 93-11632 for consideration by the Computer System Security and Privacy Advisory Board.

Please also advise the Board that I am interested in orally summarizing these comments before the Board if the Board so wishes. I can be available anytime from Noon June 2, through 1pm June 4 for this purpose.

This commentary responds to topics: 1, 2, 3, 4, 5A and (implicitly:) 6.

-
1. Cryptographic Policies and Social/Public Policy Issues
 2. Legal and Constitutional Issues
 3. Individual Privacy

Assuming Clipper technology lives up to its promise, it is encouraging to realize that the threat of covert secret "backdoors" — as has been conjecturally feared in other government-proposed algorithms — is replaced by a rational and well-understood split-key escrowing mechanism by which the system can be legally and selectively penetrated.

Clipper appears to be an attempt to balance the desire for private communications against society's perceived need to defeat privacy in order to protect itself from criminals.

Were legislation prohibiting encryption in any way ever to be proposed, it should be vigorously opposed. Such a law would infringe on First Amendment rights of free expression; of formulating a message as the author sees fit — which includes the right to twist, contort or otherwise scramble one's own message as desired.

There has always been the ability, if not the right, even before computers, to embed secret code words or other gimmicks in a message. Properly done, this is difficult to detect — much less to enforce. In the computer age, there are even better ways to covertly embed secret information in an otherwise innocuous message. Even in a draconian society that prohibited computer encryption, one could hide an encrypted message by, say, scattering its bits according to some agreed-on rule sparsely throughout a digitized graphical image. One can easily imagine software that would do this automatically. Those who wish to use encryption can always find ways to do so covertly.

As a practical matter, it seems that a free, stable, democratic government must be perpetually engaged in searching for the proper balance between the anarchy of absolute individual freedom versus the need to minimally curtail such freedom in order to prevent its unlawful criminal abuse in ways that would harm society.

It seems entirely justified that the Federal government stipulate the type of encryption, such as Clipper, it deems appropriate in conducting and protecting its business. So long as other types of encryption are not outlawed, it also seems justified that private industry be allowed, even encouraged, to implement Clipper encryption into technology offered to the general public.

As a life-long advocate of encryption, I have always felt that on balance the use of encryption gives net overall benefit to society. Encryption is embodied in many of the products Fischer International produces. It is a valuable tool to protect trade secrets, confidential information, and intellectual property against theft and conversion. However, I am also acutely aware that, like any powerful tool, encryption can be misused toward evil ends. This possibility has always caused me some concern — just as I presume vendors of hypodermic needles or weapons must be concerned about the misuse of their products.

Use of Clipper technology may help ease these qualms and, in this age of burgeoning wireless communication, encourage encryption in commercial products where it is needed to protect the privacy of citizens and enterprises. Clipper appears to permit this without creating a shield impervious to law enforcement.

Technically, Clipper appears to be a reasonable balance between privacy needs and government law enforcement needs.

However, there remain a number of critical unresolved issues regarding its general use, including:

- How to effectively safeguard against possible abuse or compromise of the escrowed key-halves. These include technical, legal and societal safeguards.

In formulating policy, it is imperative to remember history's most recurrent lesson: that money and power are enormously strong corrupting influences.

Tomorrow's communications traffic, given an appropriate vantage point, may be even easier than today's to monitor and intercept.

We must therefore choose our escrow agents wisely, guarding against at least three threats:

- That some cabal of cronies at the highest levels of a future government could corrupt the escrow process and use this to enhance and perpetuate their own power or political goals.

We must ensure that there can never be a "Clipper-gate."

- The danger that "friends in high places" could be used by private corporations to intercept and decode sensitive commercial messages, such as bids transmitted and "sealed" with Clipper, for their own interests.

While not precisely identical, it is cautionary to recall that the French government is known to have given their domestic enterprises an advantage by supplying them with government-intercepted messages containing competitors' trade secrets and intellectual property.

- If the day comes that society — industry, government, law enforcement, and citizens together — takes for granted privacy based on Clipper, then an organized attack by a relentless, patient and powerful opponent — such as a hostile foreign government or an organized international crime syndicate — may be able to subvert or coerce specific individuals who wield access to the various split-key escrow repositories.

Incidents such as the Walker spy scandal serve to remind us how little money is sometimes required to corrupt a few key individuals. One can envisage situations in which access to escrowed keys might yield great financial rewards — potentially making available lucrative bribes.

And what will be the penalty for falsely disclosing escrow keys? Will it be death for treason? prison for a criminal charge? A civil fine? Or simply dismissal?

We must carefully ascertain the possible risk/reward that will someday be presented to escrow guardians.

Splitting escrow keys helps immensely. One might argue they should be split more than two ways.

- The Clipper algorithm is secret and cannot be embodied in software. This is apt to inhibit its use in general purpose applications.

There will be a market for special-purpose security software to exploit Clipper. Initially this will be aimed at satisfying Federal government needs.

However, with general purpose software, such as office automation, or word processing, or spreadsheets, or utilities, it seems unlikely that Clipper can be used as other than a possible optional feature:

- In general, mass market software strives to exclude as few platforms as possible. The larger the market base, the better.

- When encryption is useful, then relying solely on Clipper excludes a large population.
- Thus vendors must offer a software alternative, such as DES, RC4, or some proprietary encryption algorithm to customers unwilling to invest in Clipper-enriched hardware.
- To the degree that interchange of encrypted data is done, one expects the "least common denominator" to prevail — i.e., software encryption, probably with DES.

DES is a fully documented standard, well respected and trusted in the commercial marketplace. It is flexible and can be implemented in both hardware and software.

Clipper is secret and can only be accessed through hardware.

It is instructive to observe that even after being a standard for roughly 15 years, DES hardware is accessible to only a small minority of all computer users. One ventures that the bulk of all computers using DES do so in software.

- Because, presumably, the Clipper escrow agents will be subject to control by the U.S. Federal government, it is unclear how this technology can possibly be accepted in foreign markets.

Hypothetically turning the tables for a moment: would it be a wise policy for an American company to buy communications encryption equipment that was known to have trapdoors subject to being operated only by a foreign government? How could this be prudent? What American company would feel comfortable making a big investment in such technology? Could such technology become widespread in the U.S.? Could I use it interoperably?

I believe that foreign markets will therefore be compelled to view Clipper suspiciously. And in its current instantiation, it will surely be rejected. Clipper will be stigmatized and avoided even in applications for which it may be actually suited. I see several eventualities:

- Desire for encryption continues to increase — everywhere we see increased need to protect communications (tabloids show how easily even the privacy of foreign royalty can be breached).
- As world commerce and communications become more tightly knit, U.S. companies will continue to increase their use of encryption.

- For software, especially software such as electronic mail, it seems likely that DES or RC4 will continue to be the favored encryption method — if only because they can be processed universally without extra hardware. DES encryption is certainly available throughout the world (e.g., there are companies in Switzerland, Israel and Moscow that freely market RSA and DES software — even hardware). These vendors have gained increasingly strong footholds — at least in part, I believe, due to the constraints placed on American companies through the ITAR.

Since RSA and DES software is readily available elsewhere, Americans can interoperably communicate with foreign clients, suppliers and partners using common standard protocols (such as PEM and ISO/CCITT X.400 and X.500) based on these algorithms — even though American vendors will be discouraged from supplying the software on both sides.

- Clipper may become standard for U.S. telephonic encryption. However, it is doubtful this can happen worldwide. There is a danger that Clipper will fizzle and foreign vendors will step up exports of, say, DES-based systems with world-wide interoperability.
- However, for at least telephony, interest in domestic-only privacy will probably overwhelm concerns about international compatibility, so that Clipper will gain foothold as a US standard.
- If this does occur, which I believe is the most likely scenario, then telephonic encryption may well evolve worldwide into separate incompatible nationalistic pockets.
- Of course, as callers become accustomed to domestic privacy, they will be more sensitive to its absence in international communication.

Secure international communication may be relegated to use of secure electronic mail. Alternatively, it may create a niche market for vendors (from non-export-controlled countries) of DES-based telephone equipment for international communication.

Putting Clipper under ITAR munitions license probably assures that products using it will positively never be accepted by foreign markets.

However it may tend to prevent foreign manufacturers from buying and exporting the chips for incorporation into finished products, such as telephones, to be sold into the U.S., and therefore, serve to protect U.S. vendors.

If Clipper was only subject to Commerce jurisdiction, then it still seems doubtful that it would be accepted in foreign markets; however, it probably allows foreign competition to buy Clipper chips for inclusion into products resold in the US.

Responsive answers to the issues posed by (4):

4.A Industry Views on U.S. Export Controls

Export controls are estimated to have cost Fischer International millions of dollars in lost revenue for cryptographic products.

Only a fraction of the total loss can be measured by direct customer rejection. A far greater loss has come from lost sales opportunities. Distributors are reluctant to get involved with the paperwork and delays of exporting under ITAR. This reason has been repeatedly cited.

We have also been inhibited from directly selling to foreign end users due to the exorbitant paperwork for each one.

For example, after a long and arduous selection process, our Watchdog PC data security product was chosen by a particular foreign government to become their security standard — provided we could supply the DES version.

Ultimately, an export license for DES was not granted and we lost the business. This cost us roughly \$400,000 in the immediate order; and untold millions in ultimate ongoing and future business.

Another foreign DES-based product was ultimately selected.

This is not an isolated case. The amount of business we have lost to foreign competitors due to export restrictions is in the multiple millions.

As the pattern became clear, we obviously curtailed effort in cultivating business that we would be forbidden to fulfill.

The dollar value of overall foreign business — and opportunities — lost by our company to foreign competitors due to U.S. export restrictions is certainly in the millions — and probably in the tens of millions.

In what way does the United States benefit when we lose business in a futile charade of pretending to prevent foreign access to encryption technology?

If American software and hardware manufacturers are not permitted to supply strong encryption products to the foreign market, or if our products or supply capability are perceived as being inferior due to U.S. policies (such as key escrow or export control), then foreign suppliers will use these facts or perceptions to their competitive advantage and fill the void with their own effective cryptographic products.

As indicated, current U.S. export policy has a chilling effect on the ability of American companies to sell cryptographic products in foreign marketplaces.

DES was invented in the U.S. and has evolved into a world standard; yet American companies are prohibited from supplying this standard to most foreign customers. U.S. policy forces American producers to yield the market for this U.S. technology to foreign suppliers.

Withholding American products from these markets strengthens the existing foreign competition, and stimulates the creation of products when there otherwise may have been none.

In effect, we are not only losing business, we are losing control. We are forcing the creation of strong foreign products, and giving them a greater market share, more revenue and more profit. By allowing them to offer their international customers "corporate-wide" global solutions — while American companies are limited to offering U.S.-only solutions — we are making them stronger and giving them enormous leverage even to invade us in the domestic U.S. marketplace.

The use of cryptology is burgeoning — it is becoming an integral part of more and more software. Therefore, the current policies have the effect of sacrificing not only the U.S. security software market, but eventually a large piece of the entire software market to foreign competitors.

The ultimate effect of American export policy is to:

- Severely weaken the market position of American software suppliers — one of the few industries in which America is still strong and vital.
- Create and nurture foreign competition in an area where the U.S. presently holds a technological edge.
- Make the U.S. more dependent on foreign suppliers.
- Yet still not have the desired effect of suppressing encryption.

In the final analysis, our current American policy does not effectively stifle the use of encryption — it merely serves to guarantee that it will be supplied by foreign vendors who will come to dominate the market through a suicidal U.S. policy which makes them strong by crippling American producers.

4.C Industry View: Customer Requirements for Cryptography

Demands for encryption will continue to grow. As computing becomes more prevalent; and as more valuable information is distributed across a wider area, so will the demand for cryptographic security increase.

It will be demanded to protect:

- information flow in distributed systems;
- confidentiality of electronic mail;
- electronic commerce;
- data stored on laptops;
- operating systems from viruses;
- wireless communication;
- telephonic communication;
- distribution of copyrighted products, such as games and movies.

Ultimately most important applications will use some form of encryption and digital signatures to protect confidentiality and authenticity of data.

We use cryptology in our products to protect against a wide variety of threats, including:

- Ensuring that data on a PC or laptop is transparently encrypted making it useless to anyone except the rightful owner.
- Detecting existing virus infection.
- Protecting against the possibility of future virus infection.
- Encrypting and signing electronic mail.
- Using cryptology in our WorkFlow product to ensure that workflow processing cannot be corrupted or abused.
- Using encryption to provide for program copyright protection.
- Protecting against the introduction against Trojan horses.

- In hardware to provide boot protection so that a PC cannot be incorrectly damaged or probed.
- Managing security in a disconnected distributed system, by using cryptographically protected access control rules.
- Providing for encrypted and authenticated host access over switched lines, allowing fully confidential sessions.
- Providing for encrypted and signed Electronic Data Interchange transactions.

Watchdog, our PC security product, has the highest rating in its product class ever granted by the NCSC.

4.D Industry View: Standards

If the European Community were to announce a symmetric non-DES European Community Encryption Standard (ECES), our company would have to consider the situation very carefully. We would weigh such issues as:

- Whether it could be implemented and manufactured in a country with minimal cryptographic export restrictions;
- Whether it was a published algorithm subject to review;
- Whether it could be implemented in software;
- Whether it was free of deliberate penetration points, such as Clipper's escrowed keys;
- Whether it passed successful review by respected organizations such as NIST, NSA and RSADSI;
- Whether it survived a reasonable inspection period.

Depending on the prospects for such a standard, we would certainly consider providing it to a European market if we could arrange to produce and deliver it without encountering U.S. export restrictions.

In fact, it is quite possible that a strong ECES which affirmatively answers the above points stands a good chance of being widely accepted in the United States as a commercially preferred international standard.

If vendors could globally market ECES products, freely without export restrictions, then it becomes the leading candidate to eventually replace DES as the symmetric encryption algorithm standard — excepting possibly in specialized government-related requirements in which DES or Clipper is mandated.

5.A American Business: Threats and Security Measures

Significant threats to American business which can be addressed by encryption include:

- Loss, especially by theft, of laptop computers wherein sensitive corporate data may be compromised.
- Telephonic communications, especially cordless and cellular communications in which corporate information can be pilfered.
- The prevention of fraud in electronic commerce by use of digital signatures.
- Protection of electronic mail privacy by encryption.
- Authentication of programs to inhibit virus infection.
- Use of cryptology to provide control of the data on corporate systems that may be only sporadically connected.

Incidents include:

- Cases where executive laptops have been stolen by competitors to obtain confidential corporate plans.¹
- When the French government gave Bull confidential information which had been extracted by French intelligence from communications between IBM offices in France and the United States.²

¹ James Daly, "Laptop Thefts Spur Security Efforts," Computerworld, October 12, 1992, p. 1 ff.

Rob Kelly, "Do You Know Where Your Laptop Is?" Information Week, May 11, 1992, pp. 28-30.

² John P. Mello, Jr., "Espionage! Are the Spooks Targeting Your Business?" ISPN News, September/October, 1992, p. 1 ff.

Geof Turner, "I Spy" Computerworld, October 29, 1992, pp. 129-130.

In balance, given proper safeguards, I am inclined to favor Clipper for its (apparent) intended use of providing high-grade privacy within the U.S. phone system, and for use within the U.S. Federal government. It personally strikes me as a reasonable balance between privacy needs and government law enforcement needs.

Thank you for the opportunity to discuss these important matters.

Addison Fischer,
Fischer International Systems Corp.
Naples, Florida 33942

813-643-1500 (voice)
813-643-3772 (fax)

Internet: addison@emc2-tao.fisc.com

X.400: gn = ADDISON,sn = FISCHER,prmd = FISC,admd = TELEMAIL,cc = US

Before the
Computer System Security and Privacy Advisory Board,
National Institute of Standards and Technology,
U.S. Department of Commerce

STATEMENT OF THE COMPUTER AND BUSINESS EQUIPMENT
MANUFACTURERS ASSOCIATION (CBEMA)

May 27, 1993

CBEMA, the Computer and Business Equipment Manufacturers Association, represents the leading U.S. providers of computers, business equipment, and telecommunications hardware, software, and services. Its members generate nearly five percent of our gross national product, perform twenty percent of industrial research and development, and employ more than one million people in the United States.

In response to the solicitation of the Computer System Security and Privacy Advisory Board,¹ CBEMA herewith submits comments reflecting its views, questions, and substantial concerns regarding the recently announced "key escrow" chip and United States cryptographic policies generally. Because only a few days have been allowed for preparation of public comments, CBEMA is responding to only some of the questions set forth in the solicitation. However, CBEMA intends to address all of these issues as part of what we anticipate will be a more comprehensive series of consultations between government and industry. We think it essential that the relevant issues, including those of privacy and economic competitiveness, receive a full and open airing. We support a process designed to achieve that end.

1. 58 Fed. Reg. 28855 (May 17, 1993).

Industry recognizes the government's legitimate interest in giving law enforcement officials access to private communications for criminal investigations and the protection of national security. However, because encryption is a matter of substantial public interest, encryption issues no longer can be treated as the province of only a small circle of national security, law enforcement, and technology experts. We therefore welcome this hearing as the first step in the establishment of a comprehensive communications security policy.

The Computer Market Today

Each year the market for computer equipment and related products manufactured in the United States becomes increasingly global. During the 1970s and early 1980s, the vast majority of sales by U.S. manufacturers were domestic. Today, however, between half and two-thirds of all sales by U.S. computer manufacturers are to foreign customers. In addition, computer use increasingly occurs in the context of networks, whether they be local area (i.e., entirely within a single office) or wide area (i.e., including terminals separated from one another by thousands of miles). The next generation of information products will depend heavily upon wireless technology, raising substantial concerns about exposure to scanners and the effect of a "key escrow" chip on the relatively limited power supply of such products.

The globalization of the market for U.S. computer equipment has paralleled a revolution in information technology that has changed fundamentally the standard modes of communication. In the past, the speed and volume of communications were far less than today, and advances in communication occurred relatively slowly. Now interconnected digital networks—such as electronic mail systems, Internet, and digital telephone systems—increasingly

are relied upon for routine as well as sensitive communications. The speed and volume of telecommunication are expanding exponentially, with product cycles measured in months rather than years.

The Demand for Encryption Capability

Unfortunately, digital communications are vulnerable to interception by thieves, hackers, industrial spies, and other unauthorized parties. Thus encryption, which was once considered important principally for protecting military and diplomatic messages, has become a standard security factor for any party--commercial as well as military or governmental--that desires to ensure the privacy of its communications.

Encryption is employed for a wide variety of reasons other than a conscious effort to shield conversations about illegal activities. Common encryption uses include: preventing the pirating of commercially valuable products like pay-per-use entertainment and databases; protection of intellectual property, such as patentable information; safeguarding communications made using wireless technology (e.g., cellular phone calls) from scanner interception; preventing embezzlement or larceny of goods and funds as routine transactions are converted to electronic traffic; and transmitting personally sensitive information, such as medical files, on broadband networks. Encryption can also be used to provide security for private communications that may include illegal activities, but we believe that the incidence of this use for encryption is infrequent in comparison with other uses for encryption.

As the threats to voice and data security have increased, both the domestic and foreign markets for encryption software and hardware have risen substantially. The 1991

domestic market for all data security materials--i.e., both hardware and software--was over \$1 billion. That same year, the European market for encryption materials increased at a rate higher than that in the United States.

It is clear to industry and the U.S. government that an expansive national information infrastructure is needed to ensure that the U.S. will remain economically competitive. However, such an infrastructure will fail without the prudent security practices that allow its users to rely on data security. In the near future, all computer and communications security will rely on cryptographic techniques to allow access to systems, authorize individuals to manipulate data, ensure proper destination of transmitted information, validate the originator of communications, and provide safe administration of rules and policies of the systems involved. The use of such cryptographic techniques will become ubiquitous in these areas.

The Clipper Chip

The Clinton Administration's announcement of the government-developed "key escrow" chip raised many questions regarding the technical specifications and implementation plans for the chip. Thus far, industry and the public have been told little about the "key escrow" chip. For this reason the comments that follow may require revision when additional facts come to light.

CBEMA has many concerns and questions regarding the implementation of the "key escrow" chip program. In particular, we are troubled by issues such as:

- the impact of the program on the privacy rights of American citizens;

- whether there will be a significant foreign market for a classified encryption product developed by a U.S. intelligence agency;
- the costs associated with incorporating the chip into U.S. products, if such incorporation is possible at all;
- the inconsistent statements by Administration officials regarding the applicability of the "key escrow" chip concept to data as well as voice communications, along with the timetable for the implementation for both voice encryption and data encryption; and
- whether the Administration, in its apparent haste to implement the "key escrow" chip program, has had a full opportunity to consider the implications of the program for all affected parties.

Legal and Privacy Issues

The U.S. has reached a balance in which law enforcement and intelligence agencies are permitted to intercept the communications of citizens only when required to meet a legitimate governmental purpose. That access is governed by the Constitution, statutes, and the judicial process. Despite the rapid increase in crime, especially that requiring external coordination (e.g., illegal drug trafficking), wiretaps recently have totaled less than 1000 per year. The disturbing aspect of both the "key escrow" chip and the FBI's digital communications access proposal are that the entire communications and computing structure of the United States should be constructed with government access built in.

We assume that our government's basic instinct is to respect the constitutional rights of its citizens. Nevertheless, we are concerned that the temptation afforded by the availability of the key will prove difficult to resist.

Americans are concerned about the increased amount of information available about them. They also are concerned about the accessibility of telephone conversations. Past surveys and legislative actions indicate that in the U.S., a major public concern is government accumulation of, access to, and misuse of information. The major concern regarding private sector information practices has been that information is too easily available, that the quality is low, and that mistakes are hard to discover and to correct. "Key escrow" does not appear to address any of these concerns. In fact, we believe that private discretion in the use of encryption is more likely to be favored by the public than the "key escrow" approach.

And what of those who wish greater protection than the government chip will provide? The White House statement of April 16, 1993 indicates that there is no current intent to prohibit the use of additional encryption devices, so long as those devices are relatively weak or their keys are escrowed with the government's agents. These restrictive conditions would mean that every telephone call, electronic mailing, and fax transmission is open to interception by the government. We question whether the American people will accept such an arrangement.

Writs of assistance and general warrants, executed by British colonial authorities without the need for a showing of probable cause, were a cause of the American Revolution. These documents essentially were fishing licenses and led directly to the adoption of the Fourth Amendment to our Constitution:

The driving force behind the adoption of the Amendment, as suggested by Madison's advocacy, was widespread hostility among the former colonists to the issuance of writs of assistance empowering revenue officers to search suspected places for smuggled goods, and general search warrants permitting the search of private houses, often to uncover papers that might be used to convict persons of libel.²

The original Constitution omitted such a provision, but only because the Framers "believed the National Government lacked power to conduct searches and seizures."³ James Madison prevailed, however, and the amendment was ratified in 1791.

In 1928 the Supreme Court held in the Olmstead case that wiretapping was not subject to the Fourth Amendment.⁴ The Court stated that there was no "search" absent some physical trespass onto protected premises and that one could not "seize" a conversation. The dissenters included Justices Oliver Wendell Holmes and Louis D. Brandeis. In the words of Brandeis:

There is, in essence, no difference between the sealed letter and the private telephone message The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded and all conversations between them upon any subject . . . may be overheard.⁵

2. United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990) (Rehnquist, C.J.).

3. Id.

4. Olmstead v. United States, 277 U.S. 438 (1928).

5. Id. at 475-76.

In 1967, however, the Court discarded both rationales of Olmstead. The Court held that conversations can be seized for Fourth Amendment purposes⁶ and that physical trespass (in this instance, into a telephone booth) is not a prerequisite for Fourth Amendment protection.⁷

Twenty years ago, the Executive Branch took the position that no warrant was required for "national security" searches involving either domestic subversion or foreign intelligence activities.⁸ The Supreme Court subsequently rejected the domestic subversion branch of this claim.⁹ The foreign intelligence branch of the claim never has been resolved by the courts,¹⁰ but Congress has enacted the Foreign Intelligence Surveillance Act of 1978,¹¹ which arguably requires a warrant if there is a substantial likelihood that communications of a United States person will be acquired.¹² The Supreme Court has held that the Fourth Amendment, particularly its warrant requirement, is inapplicable outside the United States.¹³

6. Berger v. New York, 388 U.S. 41 (1967).

7. Katz v. United States, 389 U.S. 347 (1967).

8. The Constitution of the United States of America: Analysis and Interpretation, S. Doc. No. 16, 99th Cong., 1st Sess. 1198 (1982).

9. Id. (citing United States v. United States District Court, 407 U.S. 297 (1972)).

10. Id. at 1199 & n. 26 (citing cases).

11. Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. §§ 1801-1811).

12. 50 U.S.C. § 1802(a)(1)(B).

13. Verdugo-Urquidez, 494 U.S. at 274-75.

The same is true for border searches of mail (and presumably other communications as well) entering the United States.¹⁴

Thus, at least in a case when one or both termini of a communication lie outside our borders, it is unclear that a warrant requirement exists. The government thus might take the position that in such instances, it is entitled to obtain the escrowed keys upon a simple request and without the intervention of any court. Such a state of affairs would be unacceptable to us and to our customers.

Foreign Marketability

We have noted above the globalization of the computer market and of commerce as a whole. This in turn makes imperative the consideration of not only domestic elements but also such factors as foreign marketability, international and foreign standards, and export controls.

U.S. industry cannot export what it cannot sell abroad. Assuming that the "key escrow" chip will be exportable under U.S. export control regulations, we doubt that the product will be attractive to significant numbers of foreign buyers.

First, the "key escrow" chip algorithm was developed by NSA--an organization whose tasks include accessing private communications. This has raised significant speculation that the chip algorithm contains a "trap door" that will allow NSA to decode encrypted communications without the benefit of either a court order or the escrowed keys of which the chip's proponents make so much. The classified character of the algorithm is at least as

14. United States v. Ramsey, 431 U.S. 606, 616 (1977).

problematic as its source. The announced independent panel review thus is critical to developing confidence in this technology. The independent panel should reflect a broad cross section of U.S. industry, and the review must not be restricted artificially if it is to be credible.

Second, even if no trap door actually exists, foreign customers, who will have a choice among a variety of products, will be skeptical and will not be disposed to buy a product that contains an NSA-created, classified algorithm. Because the chip contains a government-developed, government-controlled, untested algorithm, confidence in the algorithm will be low in domestic markets and nonexistent abroad, at least until validated by respected independent experts.

Third, all communications made using the "key escrow" chip will be accessible to U.S. law enforcement agencies that obtain the keys from the escrow agents. This system will deter potential foreign buyers from purchasing products containing the "key escrow" chip because of the possibility that unauthorized parties will gain access to the keys or that U.S. agencies may decode international communications, with or without warrants. Because the Administration has not disclosed the details of the proposed "key escrow" system, it is not possible to determine whether each step of the key system, including key creation, transmission, and storage, will be attended by adequate security precautions.

We question whether foreign customers will choose an encryption product that allows access by U.S. law enforcement agencies when other encryption products are readily available. Our members' monitoring of non-U.S. customer reaction to the announcement substantiates this apprehension.

Nor will the proposed enlistment of foreign governments to the "key escrow" concept obviate this concern. For one thing, we see no reason why foreign customers will take comfort in the fact that their governments, as well as the United States, freely can intercept their communications. Also, given all that we have heard in recent years about industrial espionage conducted by foreign governments on behalf of their domestic industries, United States customers will not rest easy knowing that such governments have been given the key to their encrypted corporate communications.

Finally, encryption purchasers may not be prepared to incur the significant costs of retrofitting existing equipment or replacing software to accommodate the "key escrow" chip. The existing installed base for most encryption customers uses DES or other algorithms. Available information suggests that the "key escrow" chip will be incompatible with these algorithms and would thus require customers to retrofit or replace all existing encryption materials.

Competitiveness Issues

In addition to the problems relating to foreign marketability, we are concerned by the possible costs related to the "key escrow" chip. If the "key escrow" chip is not freely exportable, U.S. companies will have to develop or continue with two product lines—one that incorporates the chip for domestic use and another (presumably with no encryption capability or an algorithm weak enough to receive NSA's blessing for export) for foreign use. Although some large manufacturers of computer and business equipment may be able to absorb the high

cost of having two product lines, many medium-sized and small U.S. firms cannot afford such an expensive undertaking.

Moreover, if the "key escrow" chip program becomes effectively mandatory (whether by law or by the adoption of the chip as the U.S. government's procurement standard) and U.S. companies are forced to include the chip in all exportable data communications devices, U.S. companies will have to absorb the additional cost (currently estimated at twenty-five dollars per chip). Because many of the devices that would incorporate the chip are relatively inexpensive, this additional cost per unit would be significant and would give foreign manufacturers of similar devices (who would not be required to include the chip in their products) an important competitive advantage.

Applicability of Chip to Data Encryption as Well as Voice Encryption

We are told that computer and business equipment manufacturers, whose products typically transmit data rather than voice communications, need not worry about the "key escrow" chip proposal because only voice communications are involved and because the immediate concern of the agencies proposing the new chip is the ability to intercept voice communications. "Yes," we hear, "we are in a great rush to see the chip in voice transmission equipment, but don't worry, you computer companies will have ample time thereafter to discuss with us what shall be done regarding data communications."

We do not doubt the good faith of our government in advancing the "key escrow" proposal. We note, though, that the presidential directive on public encryption management, released by the White House on April 16, 1993, appears to make no distinction between voice

and data communications. From a technological standpoint, any differences between the transmission of bits of voice and bits of data rapidly are vanishing. This in turn may make it difficult to question the later use for data transmission of the device that NSA seeks to introduce so quickly for voice transmission.

Perhaps NSA can make a case for proceeding quickly in the voice context while leaving for a later day the issue of data transmission. Such a case has not yet been made, however. We support rapid attention to validating the algorithm and to publishing a detailed escrow proposal so that we can evaluate the merits of such a case.

Lack of Transparency

We also are troubled by the lack of industry and public consultation that preceded the decision to create the "key escrow" system. Indeed, we understand that not even this Board was aware of the proposal before its details appeared in the press.

We are told that opposition by U.S. industry to the "key escrow" system will be in effect an effort to "lock out" law enforcement authorities. We recognize and support the government's legitimate need to have access to some communications in order to fight crime and protect national security. However, even if domestic and foreign demand for the chip did materialize and use of the chip became widespread, law enforcement officials would find it difficult, if not impossible, to gain access to the communications of those who truly pose criminal or national security threats. The "bad guys" can and will circumvent access by law enforcement officials simply by adding another layer of encryption.

In addition, we are concerned by the secret nature of the "key escrow" chip algorithm. If the algorithm for the "key escrow" chip is classified, it must be embedded in specialized hardware. The chip may work perfectly well in some voice telephone equipment, but it will be incompatible with many other products and uses, for reasons of physical scale if nothing else. Hardware manufacturers will be unable to integrate the algorithm into the broad range of their products unless they are provided with the specifications of the algorithm. Also we do not see how it could be employed in software products requiring encryption. Even if the algorithm were publicly released to allow manufacturers to embed the algorithm in software, software is easily modified and copied, so it is unclear how the "key escrow" system would function in such cases.

U.S. and Foreign Export Controls

U.S. Controls

Although the demand for data security technology is high, the U.S. government has imposed--unilaterally for the most part--strict controls on the export of encryption items. In response to high customer demand and the inaccessibility of U.S. products, many foreign companies have begun producing software and hardware that provide encryption capability. Because most other countries have less stringent export controls on encryption hardware and software, our government's cryptographic policies and regulations effectively have created an international embargo against U.S. encryption products and fostered the development abroad of indigenous encryption production.

Before 1989, all hardware and software with encryption capability were controlled by the State Department as munitions under the Arms Export Control Act¹⁵ and the International Traffic in Arms Regulations.¹⁶ In August 1989, following years of effort on the part of industry, NSA agreed to the transfer of a handful of items to the jurisdiction of the Commerce Department under the Export Administration Act¹⁷ and the Export Administration Regulations.¹⁸ These transferred items were limited to encryption used for data authentication, password encryption, access controls, automatic teller equipment, and decryption for copy-protected software.¹⁹

Encryption devices and software capable of encrypting data transmissions²⁰ and files continue to be classified and treated by the U.S. government as munitions. NSA, which reviews encryption export license applications, routinely recommends denial of those for file and data encryption unless the items are destined for one of nine allied governments, certain foreign banks, or foreign subsidiaries of U.S. corporations. Even "mass market" software, which by definition is "sold from stock at retail selling points," is controlled as a munition if it has file or data encryption capability.

15. 22 U.S.C. § 2778.

16. 22 C.F.R. pts. 120-130.

17. 50 U.S.C. app. §§ 2401-2420.

18. 15 C.F.R. pts. 768-799.

19. See 56 Fed. Reg. 42875 (1991) (codified at 15 C.F.R. § 799.1, supp. 1, categ. 5.II.).

20. Other than data transmissions used in password and authentication functions.

Export Controls of Other Countries

In stark contrast to the controls outlined above, most foreign countries impose significantly fewer and less restrictive controls on encryption exports than does the United States. Further, encryption is not on the International (COCOM) Munitions List so there is no multilateral requirement that it be controlled as a munition.

The United Kingdom, for example, controls encryption as a dual-use item. Thus, pursuant to COCOM's General Software Note (GSN),²¹ a U.K. exporter need not obtain a validated license if its product comes within the "mass market" provisions of the GSN. Although the U.K. does control some encryption software, the Department of Trade and Industry will consider license applications on a case-by-case basis.

Japan does not control mass-market or public domain encryption software. The Ministry of Trade and Industry will consider license applications for other encryption software on a case-by-case basis. France does not control the export of public domain software.

21. The GSN applies to "software that is generally available to the public by being--

- "a. Sold from stock at retail selling points, without restriction, by means of:
 - "1. Over the counter transactions;
 - "2. Mail order transactions; or
 - "3. Telephone call transactions; and
- "b. Designed for installation by the user without further substantial support by the supplier."

15 C.F.R. § 799.1, supp. 2. When the COCOM Core List, of which the GSN is a part, was adopted in 1991, the United States objected unsuccessfully to the inclusion of the qualifier "substantial" in paragraph b.

However, exporters must receive licenses to export mass-market software, which is controlled as a military item. Germany has exempted encryption software from the GSN. Thus, like the United States, Germany controls both public domain and mass-market software. The Netherlands generally does not control public domain or mass-market software. However, the Netherlands does control exports of software that contain file encryption capability.

Impact of U.S. Controls

Because United States export controls are more restrictive than those in many other countries, U.S. cryptographic policy and regulations have had a profound adverse impact on U.S. industry. While the U.S. government has controlled strictly the export of all but the weakest forms of encryption, a highly competitive data security industry has developed overseas. Software and devices that provide encryption capability are now available from producers in many countries, including Australia, Belgium, Canada, Denmark, Germany, Israel, the Netherlands, Russia, Sweden, and the United Kingdom. Details on individual products appear in the Appendix to this document. These materials employ a variety of algorithms, including the Data Encryption Standard (DES), which is the current U.S. standard, and numerous proprietary algorithms.

Because foreign manufacturers are not subject to United States export controls, offshore encryption producers are outdistancing U.S. vendors in bringing encryption software and services to the international market. Further, U.S. manufacturers are subject to a policy of embargo for non-bank commercial customers for software providing file encryption. Foreign manufacturers are far freer to export similar products and usually are not subject to restrictions

on domestic implementation. As a result, U.S. producers must choose between exporting unprotected (and easily pirated) software or forgoing sales abroad.

Many members of CBEMA have lost significant sales due to overly burdensome U.S. export controls. For example, one company lost a \$60 million sale for network controllers and software to support encryption of financial transactions for a government-owned telephone company in a Western European country. The customer required data security as a necessary element of a large project to replace current systems and networking capacity. Because the customer would not guarantee that the encryption could be limited to financial transactions, the export license application was denied.

In addition, U.S. export controls often require companies to produce two versions of the same product--one that is acceptable for export and one for domestic use. However, a foreign-produced product functionally identical to the controlled U.S. version frequently is available in overseas markets. For example, Distributed Computing Environment (DCE) network services software provides a standards-based framework for the development, administration, and use of distributed applications. One U.S. company that manufactures and markets DCE has created two product lines--a domestic version containing user accessible file/data encryption capability and an international version with the user accessible cryptographic functionality removed. Beyond the extra costs involved in packaging, promoting, and distributing two versions of the same product, the company has difficulties supporting its product because it cannot export the source code without a munitions license and because of incompatibility with other DCE versions.

Despite the impact on U.S. industry, export controls on encryption materials might be defensible if the controls prevented the spread of sensitive technology. However, U.S. controls frequently have no effect other than preventing U.S. sales abroad. For example, one U.S. vendor had to ship a system stripped of cryptographic functions to a foreign manufacturer. The foreign manufacturer added the missing functionality from a non-U.S. source. The manufacturer then could sell to foreign customers the identical product the U.S. vendor produced for the U.S. market but could not sell to the foreign market.

Foreign Import Controls

Absent the U.S.'s overly restrictive controls, there would be few if any obstacles to sales of U.S. encryption products in most foreign countries. Most countries (including Belgium, Brazil, Germany, Italy, Malaysia, the Netherlands, Spain, Sweden, Switzerland, Taiwan, Thailand, and the United Kingdom) impose no import restrictions for encryption materials. Some foreign countries, on the other hand, almost certainly will forbid the import of the chip unless they are given the keys and a full description of the algorithm. France is most notable, but likely not alone, in this regard.

We know of five countries that exercise import restrictions--i.e., that require an import permit or license--for encryption hardware or software. These are Australia, France, Hong Kong, Israel, and Singapore. Australia requires an import certificate only upon request by the exporting country. France requires DES-based encryption manufacturers and users to deposit a key with the French government and may also require an import permit if determined necessary under a case-by-case review. Although Israel and Hong Kong impose import

restrictions on encryption, the scope of their restrictions is not clear. Singapore will allow the importation of DES-based software for banking applications but requires a case-by-case review for all other applications.

Of the five countries that impose import restrictions, none absolutely prohibits the importation of encryption items. Most restrict importations of encryption devices and software only in limited circumstances and allow for case-by-case review. Such review, however, would be far too costly for manufacturers of relatively low-cost, high-volume items such as personal computers.

* * *

In conclusion, neither our government nor the private sector nor other governments can return to the past. Instead of giving a preferred position to one "key escrow" proposal, we must work together to fashion policies supportive of a national information infrastructure, the rights of our citizens in a technological society, and law enforcement/national security needs in the 1990s. We have learned enough to understand that not enough is known. While this hearing will provide data for both the Board and the public, no decisions can be made on the specific "key escrow" proposal, let alone on the overall character of cryptographic policy, until additional information is forthcoming from the government.

Members of the Computer and Business Equipment Manufacturers Association:

3M

AMP Incorporated

Apple Computer, Inc.

AT&T

Bell & Howell

Bull HN Information Systems, Inc.

Compaq Computer Corporation

Dictaphone Corporation

Digital Equipment Corporation

Eastman Kodak Company

Fujitsu America, Inc.

Hewlett-Packard Company

Hitachi Computer Products (America), Inc.

Honeywell Keyboard Division

IBM Corporation

Information Handling Services

Lexmark International, Inc.

Multigraphics, A Division of AM International, Inc.

NCR Corporation

Panasonic Communications & System Company

Smith Corona Corporation

Sony Corporation of America

Tandem Computers Incorporated

Tektronix, Inc.

Xerox Corporation



WASHINGTON OFFICE

122 Maryland Ave., N.E.
Washington, D.C. 20002
(202) 544-1651

Laura Murphy, Esq.
Executive Director

National Headquarters
139 West 43rd Street
New York, N.Y. 10036
(212) 544-3600

Reading Room
139 West 43rd Street

Mr. Glazer
Executive Director

May 28, 1993

Cryptographic Issue Statements
Computer System Security and Privacy Advisory Board
Technology Building
Room B-154
National Institute of Standards and Technology
Gaithersburg, MD 20899

The American Civil Liberties Union (ACLU) submits the following comments to the Computer System Security and Privacy Advisory Board in response to its pre-publication notice of comments dated May 13, 1993, regarding the Administration's "Clipper Chip" proposal.

The ACLU is a non-profit, private organization with over 275,000 members dedicated to the preservation of the Bill of Rights. The ACLU has long worked to protect civil rights and civil liberties, including the rights of privacy and free speech.

The following comments are not exhaustive, but were prepared in the very short time period between the solicitation for these comments and their due date. The issues raised are both numerous and complex and thus the comments that follow outline our concerns but do not address them in detail. However, we are in the process of working with the Digital Privacy and Security Coalition, comprised of industry and advocacy groups preparing a more thorough, in-depth discussion of the constitutional, legal and policy issues posed by the proposal.

The ACLU is concerned that government policies related to public key encryption in general and to its recently announced Clipper Chip initiative raise serious constitutional problems under the First, Fourth and Fifth Amendments that have been insufficiently addressed in the past. We believe the constitutional questions must be addressed before the initiative goes forward. Further, there are legal issues under the Electronic Communications Privacy Act (ECPA) and public policy concerns to address as well. We start with some basic and perhaps obvious premises that bear repeating.

Recent technological advances permit individuals to communicate faster and more frequently and provide access to

This is 100% recycled paper

195

enormous amounts of information quickly and cheaply. Such communications and information sharing are fundamental free speech activities protected by the First Amendment whether they take place over new telecommunications and computer technologies or in code. At the same time, these new technologies threaten to erode individuals' privacy by making possible the rapid and inexpensive amassing of vast amounts of personal information on others that would not have been so easily accessible in the past.

The most simple example is private communications on both computer networks and telephones. While those technologies are vulnerable to interception or overhearing by third parties without the consent of the parties to the communication, it is essential to recognize that the privacy interests in the communications and information are the same and must be equally protected as if the communications were in person or by written letters. In fact, both the U.S. Supreme Court and the Congress has recognized that people do have a reasonable expectation of privacy in most electronic communications (see, U.S. v. Katz and the Electronic Communications Privacy Act of 1986).

Indeed, while technology makes such invasions of privacy possible, new technology can also be used to protect such speech and privacy. One of the major ways in which this has been done is through the development of encryption technology that permits individuals to protect the privacy and property of their communications.

We are greatly concerned that the present Clipper Chip initiative does not give adequate recognition to the important constitutional principles at stake, but instead erodes them. As we understand it, the government's objective here is to hold the key to unlock any encrypted voice or data communication. (It appears that the Clipper Chip and Capstone chips together are designed for all voice and data communication.) The Administration defends the proposal as necessary for law enforcement and national security purposes, because otherwise it may find itself in the position of executing a warrant to intercept a communication but being unable to decode encrypted communications on a real time basis or perhaps ever. The Administration presently describes the proposal as "voluntary," claiming that it does not presently seek to outlaw domestic use of encryption where it does not hold the key, but rather intends to use its overwhelming market power to drive out any alternatives.

Nevertheless, the ACLU believes that there are important unresolved issues concerning the degree of government coercion involved in this proposal. It is clear that the government's stated law enforcement objective can only be achieved if it ends up holding the key to substantially all encrypted communications. Otherwise, the government will have access to decipherable

communications, but serious law breakers will use other encryption devices to which the government does not hold the keys. Any scheme that is either mandatory or leads to a "de facto" universal standard has constitutional implications. But even the proposal as presently described contains legal restrictions in the form of export controls that would seem to be essential to the government's scheme, as well as the coercive use of overwhelming market power (i.e., through the use of government contracts).

First, the ACLU is disturbed about the process put in place by the Administration by announcing a major new policy initiative which it has already begun to implement without soliciting any prior public comment or review. The timetable that the Administration has announced for fully implementing its proposal is so short as to preclude adequate public study and comment.

Second, while the proposal is described as providing for "escrowed" key systems, in fact, it appears that the "escrow" holders will be either government agencies or agents and therefore, the traditional legal notions of independent escrow agents with fiduciary obligations to both parties will not apply. The term "escrow" would seem to obscure rather than illuminate the government's role here.

Third, while the ACLU recognizes the importance of both effective law enforcement and protecting true national security interests, we have long pointed out that one of the costs of living in a free and democratic society is that neither law enforcement nor national security can be protected at any cost. Some balance must be struck between the two. We do not believe that the government has yet established a sufficient justification for its unprecedented key escrow scheme on either law enforcement or technical grounds. It has not shown that its present inability to decrypt encoded communications or data has had a serious deleterious effect on either law enforcement or national security interests. Nor has it established that this system is the only technical solution: that relying on traditional warrant procedures it would not be able to obtain most of the evidence that it requires.

Fourth, any prohibition on encrypted communications, including one that restricts such communications unless the government holds the key, raises substantial First Amendment problems. Such a prohibition on encrypted speech is a direct restriction on speech and we do not believe that the government may, in effect, ban all encrypted speech, because encrypted speech that is evidence of crime may be unobtainable. There are other First Amendment problems including the issues regarding export controls outlined below as well as the propriety of classifying the algorithm used for the Clipper Chip.

Fifth, there are serious Fourth and Fifth Amendment problems in requiring disclosure of the key to the government in advance of there being probable cause sufficient to entitle the government to seize an encrypted communication and to search and seize the key to such communication. In this connection, we believe that a case has not yet been made about why traditional warrant procedures will be insufficient to obtain evidence of criminal activity when such evidence is encrypted.

We also note that a crucial distinction must be made between seizure of encrypted conversations and seizure of encrypted documents or papers. The Fourth Amendment prohibits secret searches of an individual's papers. This means that the government, through the warrant procedure, must give an individual notice that her papers are to be searched or seized. The law has approved only one exception to the prohibition on secret searches, namely the real-time seizure of conversations without notifying the parties that their conversations are being overheard. Even then, under Title III of the U.S. code, they must usually be given subsequent notification. The rationale for this exception is the ephemeral nature of conversations -- if the parties knew they were being overheard, they would not have the conversations in the first place. Thus, it is important in evaluating the government's asserted need for a pre-warrant code-breaking ability, to recognize that it has no right to the secret seizure of "papers" or electronically stored documents, but must notify the owner that documents are being seized at the time.

Sixth, the ACLU asserts that the present system of export controls on cryptography is unconstitutional. The government has imposed export controls on cryptography software and algorithms, even when those exist in the public domain and were in no way developed by the government. This technology is speech protected by the First Amendment and the government must meet strict First Amendment standards before imposing such a licensing scheme, which is essentially a prior restraint that operates as censorship. We do not believe those standards have been met.

Moreover, we are distressed that the government appears to take the position that because such speech can be encoded onto a computer disk, it somehow loses First Amendment protection, and can be regulated in the same fashion as weapons hardware. The present export system is objectionable on its own and, as an essential element of the Clipper Chip initiative, makes that proposal even more problematic.

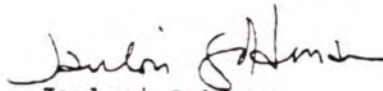
Finally, there is the broader aspect of individual privacy rights. The Administration describes the initiative as an effort to protect individual privacy, when in fact its sole purpose is to make sure that all communications are accessible to the government and cannot remain private outside the scope of government decryption.

We appreciate the opportunity to submit these comments. We urge the Advisory Board to recommend to the Administration that the Clipper Chip initiative be delayed until a serious examination of the legal and policy issues is undertaken and the critical questions resolved. In this regard, we believe it is imperative that the Administration involve the Digital Privacy and Security Coalition in this process. We look forward to providing you with more detailed comments in the near future.

Sincerely,



Kate Martin
Director, Center for
National Security Studies



Janlori Goldman
Director, ACLU Privacy
and Technology Project

NON-CERTIFIED TEXT

COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

RESOLUTION #1

June 4, 1993

At Mr. Kammer's request we have conducted two days of hearings. The clear message of the majority of input was that there are serious concerns regarding the Key Escrow Initiative and the Board concurs with these concerns. Many of these issues are still to be fully understood and more time is needed to achieving that understanding.

Accordingly, this Board resolves to have an additional meeting in July 1993 in order to more completely respond to Mr. Kammer's request and to fulfill its statutory obligations under P.L. 100-235. The Board recommends that the inter-agency review take note of our input collected, our preliminary finding, and adjust the timetable to allow for resolution of the significant issues and problems raised.

Attached to this resolution is a preliminary distillation of the serious concerns and problems.

Attachment

FOR: Gallagher, Gangemi, Lambert, Lipner, Kuyers, Rand,
Whitehurst, and Zeitler

AGAINST: none

ABSTAIN: none

NON-CERTIFIED TEXT

COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

ATTACHMENT TO RESOLUTION #1

June 4, 1993

- A convincing statement of the problem that Clipper attempts to solve has not been provided.
- Export and import controls over cryptographic products must be reviewed. Based upon data compiled from U.S. and international vendors, current controls are negatively impacting U.S. competitiveness in the world market and are not inhibiting the foreign production and use of cryptography (DES and RSA).
- The Clipper/Capstone proposal does not address the needs of the software industry, which is a critical and significant component of the National Information Infrastructure and the U.S. economy.
- Additional DES encryption alternatives and key management alternatives should be considered since there is a significant installed base.
- The individuals reviewing the Skipjack algorithm and key management system must be given an appropriate time period and environment in which to perform a thorough review. This review must address the escrow protocol and chip implementation as well as the algorithm itself.
- Sufficient information must be provided on the proposed key escrow scheme to allow it to be fully understood by the general public. It does not appear to be clearly defined at this time and, since it is an integral part of the security of the system, it appears to require further development and consideration of alternatives to the key escrow scheme (e.g., three "escrow" entities, one of which is a non-government agency, and a software based solution).
- The economic implications for the Clipper/Capstone proposal have not been examined. These costs go beyond the vendor cost of the chip and include such factors as customer installation, maintenance, administration, chip replacement, integration and interfacing, government escrow system costs, etc.
- Legal issues raised by the proposal must be reviewed.
- Congress, as well as the Administration, should play a role in the conduct and approval of the results of the review.

NON-CERTIFIED TEXT

COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

RESOLUTION #2

June 4, 1993

Key escrowing encryption technology represents a dramatic change in the nation's information infrastructure. The full implications of this encryption technique are not fully understood at this time. Therefore, the Board recommends that key escrowing encryption technology not be deployed beyond current implementations planned within the Executive Branch, until the significant public policy and technical issues inherent with this encryption technique are fully understood.

FOR: Gangemi, Lambert, Lipner, Kuyers, Rand, Whitehurst, & Zeitler

AGAINST: Gallagher

ABSTAIN: none

The New York Times

Panel Sees Flaws in Plan For Encoding

By JOHN MARKOFF

Special to The New York Times

SAN FRANCISCO, June 4 — A Commerce Department advisory committee issued two draft resolutions today raising "serious concerns" about a Clinton Administration plan to standardize a high-technology coding system that would permit law enforcement officials to tap telephone calls and computer data transmissions.

The resolutions call on the Administration to hold extensive public hearings on the new technology, known as the Clipper chip, and they urge that the technology not be deployed beyond the executive branch of the Government until the public review is completed.

The Computer System Security and Privacy Advisory Board, which was established by Congress under the Computer Security Act of 1987, held two days of public hearings this week to solicit industry and public reaction to the plan, which would create a national standard for telephone and data coding. The system would permit law enforcement officials to create a numeric "master key" that would be held in "escrow." It could be obtained only by presenting a warrant to two separate agencies that would be charged with protecting pieces of the key.

Splitting the Key

The idea is that splitting the key would make it more difficult for Government officials or other people to abuse its powers.

But the proposal has generated widespread criticism from technology experts, industry officials and privacy advocates who argue that it is technically flawed and that it holds out the possibility of widespread abuse by Government officials and others. A number of industry executives and opponents of the plan said that today's resolution was a setback for the Government.

"This is a victory for the private sector and the privacy community," said Marc Rotenberg, Washington director of the Computer Professionals

New Review Urged for Plan

Continued From First Business Page

for Social Responsibility, a computer industry public interest group. "The board heard a strong set of witnesses this week saying, 'Don't do it.'"

A White House official, who spoke on the condition of anonymity, said today that the Administration was comfortable with the resolution and that the Government was not rushing to put its plan into effect.

"People are nervous that we're immediately going to go out and procure 10 million of these devices," he said. "That's not the case. We're engaged in our own review that will go on through the summer."

The Government plan calls for the use of several chips, known as Clipper and Capstone, designed by the National Security Agency to encode voice and data conversations, but it will not outlaw the use of other coding systems. This has led many critics of the plan to argue that the proposed coding technology will not be useful in listening to people suspected of criminal activities who wish to protect their conversations.

Today's resolutions raise a number of questions about the new surveillance technology. The advisory board says that it sees these shortcomings in the proposal:

¶The Administration has not made a persuasive argument that a significant problem exists that Clipper will try to solve.

¶Because it is a hardware-based solution, the Clipper/Capstone proposal does not address the needs of the software industry.

¶Sufficient information must be provided on the proposed escrow plan to allow it to be fully understood by the general public.



Digital Telephony

Digital Telephony



**DIGITAL TELEPHONY
SUMMARY OF ISSUES**

- ♦ The FBI utilizes electronic surveillance (wire taps) in virtually every area of its investigative responsibilities.
- ♦ The telecommunications industry, which remained virtually unchanged for approximately 50 years, is now rapidly changing to address the need for more advanced telecommunications systems, i.e., personal communications networks, advanced cellular, integrated services digital networks (ISDN) which has the capacity for high speed transmissions of video, voice and data.
- ♦ One of the telephone telecommunication industry's major developmental efforts is to provide total digital connectivity (end to end) for their subscribers, to include residential and business communities, in the near future.
- ♦ At present, no capability exist to intercept ISDN (digital) transmissions; therefore, the emergence of digital telecommunications technology will preclude the FBI and all of law enforcement from being able to intercept electronic communications thus all but eliminating a statutorily sanctioned, court authorized and extraordinarily successful investigative technique.
- ♦ The Department of Justice and the FBI have been working with the White House, other various Administration agencies, the telecommunications industry and Congress to find a workable solution to this very serious problem which endangers the safety of the American public. A legislative solution has been developed to ensure that the legitimate need for law enforcement to lawfully intercept communications is met by the telecommunication industry.

DIGITAL TELEPHONY
LEGISLATIVE REMEDY

The proposal would amend the Communications Act of 1934 to require providers of electronic communications services and private branch exchanges to ensure that the Government's ability to lawfully intercept communications is unimpeded by the introduction of advanced digital telecommunications technology or any other emerging telecommunications technology. Specifically, the amendment provides the following:

1. The FCC, in consultation with the Attorney General, shall determine the technological interception needs of the Government and issue regulations which will preserve the Government's ability to conduct lawful electronic surveillance.
2. The FCC shall issue regulations within 120 days after enactment requiring the modification of existing telecommunications systems if those systems impede the Government's ability to conduct lawful electronic surveillance.
3. Requires compliance by service providers and private branch exchanges within 180 days of the issuance of regulations and use of non-conforming equipment is prohibited thereafter.
4. Gives FCC the authority to compensate through the rate structure telecommunication system operators under FCC jurisdiction for reasonable costs associated with required modifications of existing telecommunications equipment or technology.
5. Gives the Attorney General specific authority in addition to that already vested in the FCC to seek civil penalties and injunctive relief for non-compliance.

S. _____

Amendment No. _____
Offered by M_. _____

1 SEC. 1. FINDINGS AND PURPOSES.

2 (a) The Congress finds:

3 (1) that telecommunications systems and networks are often
4 used in the furtherance of criminal activities including
5 organized crime, racketeering, extortion, kidnapping, espionage,
6 terrorism, and trafficking in illegal drugs; and

7 (2) that recent and continuing advances in
8 telecommunications technology, and the introduction of new
9 technologies and transmission modes by the telecommunications
10 industry, have made it increasingly difficult for government
11 agencies to implement lawful orders or authorizations to
12 intercept communications and thus threaten the ability of such
13 agencies effectively to enforce the laws and protect the national
14 security; and

15 (3) without the assistance and cooperation of providers of
16 electronic communication services and private branch exchange
17 operators, the introduction of new technologies and transmission
18 modes into telecommunications systems without consideration and
19 accommodation of the need of government agencies lawfully to
20 intercept communications, would impede the ability of such
21 agencies effectively to carry out their responsibilities.

1 (b) The purposes of this Act are:

2 (1) to clarify the duty of providers of electronic
3 communication services and private branch exchange operators to
4 provide such assistance as necessary to ensure the ability of
5 government agencies to implement lawful orders or authorizations
6 to intercept communications; and

7 (2) to ensure that the Federal Communications Commission,
8 in the setting of standards affecting providers of electronic
9 communication services or private branch exchange operators, will
10 accommodate the need of government agencies lawfully to intercept
11 communications.

12 SEC. 2. Title II of the Communications Act of 1934 is amended
13 by adding at the end thereof the following new sections:

14 "SEC. ____: GOVERNMENT REQUIREMENTS.

15 "(a) The Federal Communications Commission shall,
16 within 120 days after enactment of this Act, issue such
17 regulations as are necessary to ensure that the government
18 can intercept communications when such interception is
19 otherwise lawfully authorized.

20 "(b) The regulations issued by the Commission shall:

21 "(1) establish standards and specifications for
22 telecommunications equipment and technology employed by
23 providers of electronic communication services or
24 private branch exchange operators as may be necessary
25 to maintain the ability of the government to lawfully
26 intercept communications;

1 "(2) require that any telecommunications
2 equipment or technology which impedes the ability of
3 the government to lawfully intercept communications and
4 which has been introduced into a telecommunications
5 system by providers of electronic communication
6 services or private branch exchange operators shall not
7 be expanded so as to further impede such ability until
8 that telecommunications equipment or technology is
9 brought into compliance with the requirements set forth
10 in regulations issued by the Commission;

11 "(3) require that modifications which are
12 necessary to be made to existing telecommunications
13 equipment or technology to eliminate impediments to the
14 ability of the government to lawfully intercept
15 communications shall be implemented by such providers
16 of electronic communication services and private branch
17 exchange operators within 180 days of issuance of such
18 regulations; and

19 "(4) prohibit the use by electronic communication
20 service providers and private branch exchange operators
21 of any telecommunications equipment or technology which
22 does not comply with the regulations issued under this
23 section after the 180th day following the issuance of
24 such regulations.

25 "(c) For the purposes of administering and enforcing
26 the provisions of this section and the regulations

1 prescribed hereunder, the Commission shall have the same
2 authority, power, and functions with respect to providers of
3 electronic communication services or private branch exchange
4 operators as the Commission has in administering and
5 enforcing the provisions of this title with respect to any
6 common carrier otherwise subject to Commission jurisdiction.
7 Any violation of this section by any provider of electronic
8 communication service or any private branch exchange
9 operator shall be subject to the same remedies, penalties,
10 and procedures as are applicable to a violation of this
11 chapter by a common carrier otherwise subject to Commission
12 jurisdiction, except as otherwise specified in subsection
13 (d).

14 "(d) In addition to any enforcement authorities vested
15 in the Commission under this title, the Attorney General may
16 apply to the appropriate United States District Court for a
17 restraining order or injunction against any provider of
18 electronic communication service or private branch exchange
19 operator based upon a failure to comply with the provisions
20 of this section or regulations prescribed hereunder.

21 "(e) Any person who willfully violates any provision
22 of the regulations issued by the Commission pursuant to
23 subsection (a) of this section shall be subject to a civil
24 penalty of \$10,000 per day for each day in violation.

25 "(f) To the extent consistent with the setting or
26 implementation of just and reasonable rates, charges and

1 classifications, the Commission shall authorize the
2 compensation of any electronic communication service
3 providers or other entities whose rates or charges are
4 subject to its jurisdiction for the reasonable costs
5 associated with such modifications of existing
6 telecommunications equipment or technology, or with the
7 development or procurement, and the installation of such
8 telecommunications equipment or technology as is necessary
9 to carry out the purposes of this Act, through appropriate
10 adjustments to such rates and charges.

11 "(g) The Attorney General shall advise the Commission
12 within 30 days after the date of enactment of this Act, and
13 periodically thereafter, as necessary, of the specific needs
14 and performance requirements to ensure the continued ability
15 of the government to lawfully intercept communications
16 transmitted by or through the electronic communication
17 services and private branch exchanges introduced, operated,
18 sold or leased in the United States.

19 "(h) Notwithstanding section 552b of Title 5, United
20 States Code or any other provision of law, the Attorney
21 General or his designee may direct that any Commission
22 proceeding concerning regulations, standards or
23 registrations issued or to be issued under the authority of
24 this section shall be closed to the public.

25 "(i) Definitions -- As used in this section --

1 "(1) 'provider of electronic communication
2 service' or 'private branch exchange operator' means
3 any service which provides to users thereof the ability
4 to send or receive wire, oral or electronic
5 communications, as those terms are defined in
6 subsections 2510(1) and 2510(12) of Title 18, United
7 States Code;

8 "(2) 'communication' means any wire or electronic
9 communication, as defined in subsection 2510(1) and
10 2510(12), of Title 18, United States Code;

11 "(3) 'impede' means to prevent, hinder or impair
12 the government's ability to intercept a communication
13 in the same form as transmitted;

14 "(4) 'intercept' shall have the same meaning as
15 set forth in section 2510(4) of Title 18, United States
16 Code;

17 "(5) 'government' means the Government of the
18 United States and any agency or instrumentality
19 thereof, any state or political subdivision thereof,
20 the District of Columbia, and Commonwealth of Puerto
21 Rico; and

22 "(6) 'telecommunications equipment or technology'
23 means any equipment or technology, used or to be used
24 by any providers of electronic communication services
25 or private branch exchange operators, which is for the

1 transmission or receipt of wire, oral or electronic
2 communications."

3 SEC 3. Section 510, Title V, P.L. 97-259 is amended deleting the
4 phrase "section 301 or 302a" and substituting the phrase "section
5 301, 302a, or ____."

6

DIGITAL TELEPHONY AMENDMENT
(Report Language)

Significant changes are being made in the systems by which communications services are provided. Digital technologies, fiber optics, and other telecommunications transmission technologies are coming into widespread use. These changes in communications systems and technologies make it increasingly difficult for government agencies to implement lawful orders or authorizations to intercept communications in order to enforce the laws and protect the national security.

With the assistance of providers of electronic communication services, these technological advances need not impede the ability of government agencies to carry out their responsibilities. This bill would direct the Federal Communications Commission (FCC) to issue standards ensuring that communications systems and service providers continue to accommodate lawful government communications intercepts. The regulations are not intended to cover federal government communications systems. Procedures already exist by which the Federal Bureau of Investigation may obtain federal agency cooperation in implementing lawful orders or authorizations applicable to such systems. Further, there would be no obligation on the part of service providers or any other party to ensure access to the plain text of encrypted or other encoded material, but rather only to the communication in whatever form it is transmitted. It is thus the intent and purpose of the bill only to maintain the government's current communications interception capability where properly ordered or authorized. No expansion of that authority is sought.

ANALYSIS

Subsection 2(a) and (b) would require the Federal Communications Commission (FCC) to issue any regulations deemed necessary to ensure that telecommunications equipment and technology used by providers of electronic communications services or private branch exchange operators will permit the government to intercept communications when such interception is lawfully authorized. The regulations would also require that equipment or technologies currently used by such providers or operators that impede this interception ability not be expanded so as to further impede such ability until brought into compliance with the regulations. Compliance with FCC regulations issued under this section would be required within 180 days of their issuance.

Subsection 2(c) provides that the Commission's authority to implement and enforce the provisions of this section are the same as those it has with respect to common carriers subject to its jurisdiction.

Subsection 2(d) would give the Attorney General the authority to request injunctive relief against non-complying service providers or private branch exchange operators.

Subsection 2(e) provides civil penalty authority for willful violations of the regulations of up to \$10,000 per day for each violation.

Subsection 2(f) would permit the FCC to provide rate relief to service providers subject to its rate-setting jurisdiction for the costs associated with modifying equipment or technologies to carry out the purposes of the bill.

Subsections 2(g), (h), and (i) require the Attorney General to advise the Commission regarding the specific needs and performance criteria required to maintain government intercept capabilities, require the FCC to ensure that the standards and specifications it promulgates may be implemented on a royalty-free basis, and authorize the Attorney General to require that particular Commission rulemaking proceedings to implement the Act be closed to the public.

Subsection 2(j) provides definitions for key terms used in this section.

DRAFT

S. _____
[H.R. _____]

IN THE SENATE
[IN THE HOUSE OF REPRESENTATIVES]

M. _____ introduced the following bill; which was referred to the
Committee on _____

A BILL

To ensure the continuing access of law enforcement to the content of wire and
electronic communications when authorized by law and for other purposes.

*Be it enacted by the Senate and the House of Representatives of the United States
of America in Congress assembled,*

SEC. 1. FINDINGS AND PURPOSES.

(a) The Congress finds:

(1) that telecommunications systems and networks are often used in the
furtherance of criminal activities including organized crime, racketeering,
extortion, kidnapping, espionage, terrorism, and trafficking in illegal drugs;

(2) that recent and continuing advances in telecommunications technology,
and the introduction of new technologies and transmission modes by the
telecommunications industry, have made it increasingly difficult for government
agencies to implement lawful orders or authorizations to intercept wire and
electronic communications and thus threaten the ability of such agencies
effectively to enforce the laws and protect the national security; and

DRAFT

(3) that without the assistance and cooperation of providers of electronic communication services and private branch exchange operators, the introduction of new technologies and transmission modes into telecommunications systems without consideration and accommodation of the need of government agencies lawfully to intercept wire and electronic communications would impede the ability of such agencies effectively to carry out their responsibilities.

(b) The purposes of this Act are to clarify the responsibilities of providers of electronic communication services and private branch exchange operators to provide such assistance as necessary to ensure the ability of government agencies to implement lawful court orders or authorizations to intercept wire and electronic communications.

SEC. 2. (a) Providers of electronic communication services and private branch exchange operators shall provide within the United States capability and capacity for the government to intercept wire and electronic communications when authorized by law:

(1) concurrent with the transmission of the communication to the recipient of the communication;

(2) in the signal form representing the content of the communication between the subject of the intercept and any individual with whom the subject is communicating, exclusive of any other signal representing the content of the communication between any other subscribers or users of the electronic communication services provider or private branch exchange operator, and including information on the individual calls (including origin, destination and other call set-up information), and services, systems, and features used by the subject of the interception;

DRAFT

(3) notwithstanding the mobility of the subject of the intercept or the use by the subject of the intercept of any features of the telecommunication system, including, but not limited to, speed-dialing or call forwarding features;

(4) at a government monitoring facility remote from the target facility and remote from the system of the electronic communication services provider or private branch exchange operator;

(5) without detection by the subject of the intercept or any subscriber; and

(6) without degradation of any subscriber's telecommunications service.

(b) Providers of electronic communication services within the public switched network, including local exchange carriers, cellular service providers, and interexchange carriers, shall comply with subsection (a) of this section within eighteen months from the date of enactment of this subsection.

(c) Providers of electronic communication services outside of the public switched network, including private branch exchange operators, shall comply with subsection

(a) of this section within three years from the date of enactment of this subsection.

(d) The Attorney General, after consultation with the Department of Commerce, the Small Business Administration and the Federal Communications Commission, as appropriate, may except from the application of subsections (a), (b) and (c) of this section classes and types of providers of electronic communication services and private branch exchange operators. The Attorney General may waive the application of subsections (a), (b) and (c) of this section at the request of any provider of electronic communication services or private branch exchange operator.

(e) The Attorney General shall have exclusive authority to enforce the provisions of subsections (a), (b) and (c) of this section. The Attorney General may apply to

DRAFT

the appropriate United States District Court for an order restraining or enjoining any violation of subsection (a), (b) or (c) of this section. The District Courts shall have jurisdiction to restrain and enjoin violations of subsections (a) of this section.

(f) Any person who willfully violates any provision of subsection (a), of this section shall be subject to a civil penalty of \$10,000 per day for each day in violation. The Attorney General may file a civil action in the appropriate United States District Court to collect, and the United States District Courts shall have jurisdiction to impose, such fines.

(g) Definitions — As used in subsections (a) through (f) of this section —

(1) 'provider of electronic communication service' or 'private branch exchange operator' means any service or operator which provides to users thereof the ability to send or receive wire or electronic communications, as those terms are defined in subsections 2510(1) and 2510(12) of Title 18, United States Code, respectively, but does not include the government of the United States or any agency thereof;

(2) 'communication' means any wire or electronic communication, as defined in subsections 2510(1) and 2510(12), of Title 18, United States Code;

(3) 'intercept' shall have the same meaning as set forth in section 2510(4) of Title 18, United States Code; and

(4) 'government' means the Government of the United States and any agency or instrumentality thereof, any state or political subdivision thereof, the District of Columbia, and any commonwealth, territory or possession of the United States.

DRAFT

DIGITAL TELEPHONY AND INTERCEPTION
BY
CRIMINAL LAW ENFORCEMENT AGENCIES

The telecommunications systems and networks are often used to further criminal activities including white collar and organized crime, racketeering, extortion, kidnapping, espionage, terrorism, and trafficking in illegal drugs. Accordingly, for many years, one of the most important tools in the investigation of crime for Federal and State criminal law enforcement agencies has been the court authorized interception of communications. As illustrated below, the majority of original authorizations to intercept wire or electronic communications are conducted by State criminal law enforcement agencies.

Interception Applications Authorized			
	State	Federal	Total
1984	512	289	801
1985	541	243	784
1986	504	250	754
1987	437	236	673
1988	445	293	738
1989	453	310	763
1990	548	324	872
Total	3,440	1,945	5,385

Approximately, 3/8 of authorized interceptions were conducted by Federal agencies, while 5/8 of the authorized interceptions were conducted by State criminal law enforcement agencies.¹

The recent and continuing advances in telecommunications technology, and the introduction of new technologies by the telecommunications industry, have made it increasingly difficult for government agencies to implement lawful orders or authorizations to intercept wire and electronic communications, as well as to implement pen register and trap-and-trace court orders or authorizations. These new technologies inadvertently undermine the ability of criminal law enforcement agencies to enforce effectively the criminal laws and protect the national security. Without the assistance and cooperation of the telecommunications industry, these new technologies will impede the ability of the government to enforce the criminal law. Accordingly, the purpose of this bill is to clarify the

¹ Interceptions for foreign intelligence and counterintelligence purposes are not counted within the figures used here, but would likewise benefit from enactment of the legislation.

DRAFT

DRAFT

- 2 -

existing responsibilities of electronic communication services providers and private branch exchange operators, as established, for example, in 18 U.S.C. §§ 2518(4), 3124(a), (b), to provide such assistance as necessary to ensure the ability of government agencies to implement lawful orders or authorizations to intercept communications.

Over the past twenty-five years, the working relationship between the criminal law enforcement community, particularly the Federal Bureau of Investigation as the federal government's primary criminal law enforcement agency, and the telecommunications industry has been quite good. In nearly all cases, the telecommunications industry, in response to the appropriate court orders or authorizations, has provided government agencies with timely access to the signals containing the content of communications covered by the court orders or authorizations. As a general proposition, this has involved providing the means to acquire the communication as it occurs between two individual telephone users at a remote location, not dissimilar to a call in which the two originating parties do not know that a third party is listening, and in which the third party (the criminal law enforcement agency) records the authorized and relevant calls.

Historically, and with relatively few exceptions, the telecommunications industry has provided the criminal law enforcement community with the ability to monitor and record calls:

1. at the same time as the call is transmitted to the recipient;
2. in the same form as the content of the call was transmitted through the network, notwithstanding the use by the target of custom features of the network;
3. whether stationary or mobile;
4. at the government monitoring facility;
5. without detection by the target or others subscribers; and
6. without degrading any subscriber's service.

However, the introduction of new technology has begun to erode the ability of the government to fully effectuate interceptions, pen registers and trap-and-trace court orders or authorizations that are critical to detecting and prosecuting criminals. As technology has developed, the telecommunications industry has not always ensured the continued ability to provide the same services to the criminal law enforcement community. The telecommunications industry's introduction of certain types of new technology poses real problems for effective criminal law enforcement. Legislation is necessary to ensure that the government will be provided with this capability and capacity in the future by all providers and operators and to maintain a level playing field among competitive providers and operators in the telecommunications industry.

DRAFT

There have been instances in which court orders authorizing the interception of communications have not been fulfilled because of technical limitations within particular telecommunications networks. For example, as early as 1986, limited capabilities became apparent in at least one network which will only be corrected later in 1992. This technical inefficiency in a new technology forced criminal law enforcement agencies to prioritize certain interceptions to the exclusion of other court orders. Accordingly, for approximately six years, there have been court orders that have not been sought by the criminal law enforcement community or executed by the telecommunications industry and, as a consequence, important criminal investigations have not been brought to fruition or have been less than efficiently concluded. This is one classic example of new technology affecting adversely the criminal law enforcement community: a microcosm of what may be expected on a nationwide basis without enactment of this legislation.

Section 1 of the bill states Congressional findings and purpose.

Section 2 is divided into seven subsections. Subsection (a) establishes as a matter of law the responsibility of electronic communication services providers and private branch exchange operators to continue to provide, within the United States, the capability and capacity for criminal law enforcement agencies to intercept wire and electronic communications when authorized by law. These subsections delineate the existing attributes of wire or electronic communication interception.

1. Concurrent with Transmission. The application for a court order to intercept telecommunications conversations or data transmissions is rarely a leisurely process. For example, on the Federal side, the development of the required affidavits, submission to the Criminal Division of the Department of Justice for approval, transmission of approval to the Assistant United States Attorney, the appearance of the Assistant before a judge to request the order and the delivery of the judge's order to the appropriate telecommunications company is frequently completed in a very short time. However, crime waits for no one and the system for approval of interceptions must and does conform with the realities of the activity that is sought to be investigated and, if appropriate, prosecuted as criminal offenses. Since time is of the essence, current law requires that service providers and operators provide the government forthwith all information, facilities and technical assistance necessary to accomplish its mission. It is critical that the telecommunications industry respond quickly to execute the court order or authorization. The ultimate problem of timeliness, however, is the real-time monitoring of the intercepted communications. As serious and potentially life-threatening criminal conduct is detected, it may be necessary to move quickly to protect innocent victims from that conduct. Accordingly, "real-time" monitoring is critical.

2. Isolated Signal and Services Used. Nearly all of the communications network is partially "analog" at this time. In conducting an interception, for example, of a telephone conversation, the government is allowed to monitor and record criminal conversation such as a conspiracy, minimizing the acquisition of non-criminal or innocent conversation. When an electronic communication services provider or private branch exchange operator

DRAFT

introduces a new technology -- such as a digital signal -- the communications are converted into a different and more efficient form for transmission, but a more difficult form to monitor during interception. The bill requires only that the provider or operator isolate and provide access to the electronic signal that represents the content of the communications of the target of the intercept² from the stream of electronic signals representing other communications. This provision seeks to ensure that, in the new electronic environment in which signals are mixed for transmission and separated at another switch for distribution, the government does not receive the communications of any individual other than the individuals using the target's communications point of origin and receipt; the government must remain subject to the minimization standards of 18 U.S.C. § 2518(5).

This provision also makes it clear that an electronic communication services provider or private branch exchange operator is not required to provide for reconversion of the isolated communication to analog or other form. The government expects that this process will be accomplished by the government.

3. Mobility and Features. Increasingly, criminal acts are being conducted or discussed over cellular telephones or by using special telecommunications features. As this mobility is introduced, the electronic communication services providers and private branch exchange operators would be required to assure the capability and capacity for criminal law enforcement agencies to continue lawful interception.

Further, this subsection makes it clear that features used by the target do not defeat the court order or authorization. For example, communications which have been addressed to the telephone number of the target, but which may have been programmed through a call-forwarding feature to another, otherwise innocent, telephone number, must be captured and made available to criminal law enforcement authorities pursuant to court order or authorization. This requirement will obviate the need for applications for authority to monitor otherwise innocent telephone numbers that receive, only intermittently, calls forwarded by the target. The effect of this provision is to further minimize monitoring of calls of innocent parties. Similarly, certain speed dialing features that mask the telephone number called by the target must be identified for criminal law enforcement investigations. The ability to consistently determine the destination of calls is critical to minimizing the monitoring of innocent calls.

4. Government Monitoring Facility. Government agencies do not normally request the use of telecommunications industry physical facilities to conduct authorized interceptions nor is it encouraged by the industry. Normally, the government leases a line from the electronic communication services provider's or private branch exchange operator's

² Whether the content is voice, facsimile, imagery (e.g. video), computer data, signalling information, or other forms of communication, does not matter; all forms of communication are intercepted.

switch to another location owned or operated by the government. This minimizes the cost and intrusiveness of interceptions, which benefits the service provider or operator, as well as the government. Accordingly, the ability to monitor intercepted communications remotely is critical.

5. Without Detection. One of the reasons that governments operate their own facilities is to reduce the risk of detection of the interception, which would render the interception worthless. At the present time, the existence of an interception is unknown to any subscriber and is not detectable by the target, notwithstanding folklore and spy novels. This provision merely ensures that the secrecy of effective interceptions will be maintained.

6. Without Degradation. Maintaining the quality of the telephone network is in the interest of the government, the industry and the public. Presently, the existence of an interception has no effect on the quality of the service provided by any network to the target or any subscriber. This provision ensures that the quality of the network will continue to be uncompromised. Absent the assistance delineated by this legislation, the execution of court orders and authorizations by the government could well disrupt service of the newer technological systems, a result that this legislation seeks to avoid.

Subsection (b) provides that electronic communication services providers and private branch exchange operators within the "public switched network" must be in compliance with the minimum intercept attributes within eighteen months after enactment. Thereafter, new technologies must continue to meet these minimum attributes.

Subsection (c) provides that electronic communication service providers and private branch exchange operators that are not within the "public switched network" must be in compliance with the minimum intercept attributes within three years after enactment. Thereafter, new technologies must continue to meet these minimum attributes. This subsection is intended to base compliance on the capabilities of the service providers and operators who are less central to the mainstream telecommunications network.

Subsection (d) provides that the Attorney General may grant exceptions to the affirmative requirements of subsection (a), as well as the implementation deadlines of subsections (b) and (c). In considering any request for exceptions, the Attorney General will consult with the Federal Communications Commission, the Small Business Administration and the Department of Commerce, as appropriate. Accordingly, the Attorney General has the authority to except, for example, whole classes, categories or types of private branch exchange operators where no serious criminal law enforcement problems are likely to arise, such as hospital telephone systems.

This subsection also permits the Attorney General to waive the requirements of subsections (a), (b) and (c) on application by an electronic communication services provider or private branch exchange operator. Accordingly, if a particular company can not comply with one or more of the requirements of subsection (a), or needs time additional to that

DRAFT

permitted under subsections (b) or (c), the Attorney General may grant an appropriate waiver.

Subsection (e) provides that the Attorney General has exclusive authority to enforce the provisions of the bill. While a number of States have authority to seek and execute interception orders, they will be required to seek the assistance of the Attorney General if enforcement of this legislation is required. This section also provides for injunctive relief from violations of the provisions of the bill.

Subsection (f) provides for enforcement of the provisions of the bill through imposition of civil fines against any company that is not excepted from the provisions of the bill, does not acquire a waiver of the provisions of the bill, and fails to meet the requirements of subsection (a) after the effective dates set out in subsection (b) or (c), as appropriate. A fine of up to \$10,000 per day for each day in violation may be levied; for most companies in the telecommunications industry this amount is sufficient to ensure that compliance will be forthcoming. Although this provision is not expected to be used, it is critical to ensure that compliance with the provisions of the bill will occur after the effective dates of the requirements of subsection (a).

Subsection (g) carries forward a number of definitions from the current provisions for the interception of wire or electronic communications under "Title III." The definition of "government" that is currently in use includes all States, territories and possessions of the United States, as well as the United States, is made applicable to the bill.

DRAFT

GAO

Briefing Report to the Chairman,
Subcommittee on Telecommunications
and Finance, Committee on Energy and
Commerce, House of Representatives

July 1992

FBI

Advanced
Communications
Technologies Pose
Wiretapping Challenges



Information Management and
Technology Division

B-249358

July 17, 1992

The Honorable Edward J. Markey
Chairman, Subcommittee on
Telecommunications and Finance
Committee on Energy and Commerce
House of Representatives

Dear Mr. Chairman:

In March 1992, you asked us to evaluate the (1) technological alternatives available or imminently available to the Federal Bureau of Investigation (FBI) to wiretap voice and data communications,¹ (2) changes required to the telecommunications network to accommodate least intrusive wiretaps,² and (3) estimated cost of developing and implementing such changes. On June 26, 1992, we briefed your office on the results of our evaluation. At that time, we also discussed the FBI's past and current actions to satisfy its wiretapping needs, including its April 1992 proposal to amend the Communications Act of 1934 and its May 1992 proposal for separate legislation to provide for its wiretapping needs by the telecommunications industry. This report documents our briefing. Appendix I contains the slides we used at that briefing.

The FBI has classified our analysis of the technological alternatives to wiretapping as National Security Information. In this regard, we provided your office with a classified briefing on our analysis on June 15, 1992.

Results in Brief

The technological wiretap alternatives available to the FBI and the network changes needed to accommodate the least intrusive wiretaps vary depending on the technology used. However, neither the FBI nor the telecommunications industry has systematically identified the alternatives, or evaluated their costs, benefits, or feasibility.

The FBI, in its April 1992 legislative proposal, did not define its wiretapping needs. The May 1992 proposal generally addressed the FBI's needs, but did

¹Wiretapping refers to the real-time collection of dialed digits and sending of real-time, two-way communications to a listening device, regardless of the target's location or the technology used. Real time means collecting and sending this information to a listening device as it is being communicated.

²The term intrusive refers, for purposes of this report, to the level of the wiretap's detectability by the wiretap's target.

not provide specifics necessary for the telecommunications industry to determine what would constitute full compliance with the proposal in the event it were enacted. For example, the proposal did not specify the length of time allowed to install a wiretap after receipt of a court order. Further, the May 1992 proposal did not address who should pay for the cost of wiretapping solutions. FBI and industry officials have recently begun working together to identify technological alternatives available to the FBI for wiretapping and to select the alternatives that best meet their needs.

Background

The FBI considers wiretapping an essential information gathering tool in fighting crime. The federal government and 37 states have statutes governing wiretapping.

The FBI now has the technical ability required to wiretap certain technologies, such as analog voice communications carried over public networks' copper wire. However, since 1986, the FBI has become increasingly aware of the potential loss of wiretapping capability due to the rapid deployment of new technologies, such as cellular and integrated voice and data services, and the emergence of new technologies such as Personal Communication Services, satellites, and Personal Communication Numbers.

In response to the rapidly changing technology, the FBI prepared two legislative proposals in April and May 1992. The May proposal replaced the April proposal.³ According to the FBI, these proposals are intended to maintain the same level of wiretapping capability for new telecommunications technology that it has with technologies such as older analog communications using copper wire.

Technological Alternatives and Network Changes Required to Implement Least Intrusive Wiretaps Vary With the Technology

There are six current or imminent telecommunications technologies that the FBI needs to be able to wiretap. These are (1) analog and digital using copper wire transport, (2) analog and digital using fiber optic transport, (3) Integrated Services Digital Network (ISDN), (4) Private Branch Exchange (PBX), (5) broadband, and (6) cellular. There are also three future technologies for which wiretapping capabilities need to be addressed: (1) satellite switches, (2) Personal Communication Services (PCS), and (3) Personal Communication Number (PCN). Further, the FBI

³The May proposal has not been formally introduced as legislation in either the Senate or the House of Representatives.

needs to be able to wiretap any special features, such as call forwarding or electronic mail.

Wiretapping can occur at six primary locations through which the communications flow—at the premises where the target is located, between the premises and the cross-connect,⁴ at the cross-connect, or at a land line, cellular, or satellite switch.

The technological alternatives for wiretapping vary with the telecommunications technology being tapped and the location where the tap occurs. For example, the technology used to tap a nondigital telephone is different from that used to tap a digital telephone. Further, tapping at the premises may require a different technology from tapping at a switch. Similarly, the network changes needed to implement the least intrusive wiretaps vary by technology and location.

Because the FBI has classified our analysis of these alternatives as National Security Information, we are not presenting them in this report.

No Comprehensive Studies Exist Identifying Alternatives and Their Costs, Benefits, and Feasibility

As of June 30, 1992, neither the FBI nor the telecommunications industry had systematically identified the alternative approaches for implementing minimally intrusive wiretapping capabilities and the costs, benefits, and feasibility of these alternatives.

The FBI's and telecommunication industry's past efforts to identify technological alternatives have been unsuccessful. In the past, the FBI met with security officers within the telephone companies to effect wiretaps. According to the FBI and industry officials, these security officers were the designated company contacts for meeting the FBI's wiretapping needs.

However, industry security officers did not discuss the FBI's wiretapping needs with the industry's technical experts who develop the technologies. Consequently, these experts were not informed of the FBI's needs and were not involved in identifying technological alternatives and solutions until July 1990, when the FBI began technical discussions with them.

In addition, while the FBI conducted its own research on wiretapping, these research efforts were not coordinated with industry research and

⁴The cross-connect is located at the central office of the telephone company; this is where transmissions are converted from one form to another, e.g., from analog to digital.

development. As a result, neither the FBI nor the telecommunications industry had a comprehensive analysis of the technological alternatives for wiretapping current and emerging technologies.

Recent FBI Actions to Define and Communicate Its Wiretapping Needs

Recently the FBI has taken actions to better define and communicate its wiretapping needs to the telecommunications industry.

The April 1992 proposal to amend the Communications Act of 1934 did not define the FBI's wiretapping needs. In contrast, the May 1992 proposal for separate legislation, which replaced the April proposal, contains specific high-level discussion of its needs. For example, the May proposal states that tapped data must be in the same form as that received by the target and the data must be in real time, independent of the target's location, undetectable, and capable of being transmitted to a listening device. It also specifies time limits for meeting the FBI's needs and gives the Department of Justice the authority to ensure compliance or grant exemptions.

However, the May proposal does not address what the telecommunications industry would need to do to be in full compliance with the proposal in the event it is enacted, the meaning of certain technical terms, or who would pay for the cost of wiretapping solutions. For example, the proposal did not specify the length of time allowed to install a wiretap after receipt of a court order. According to the FBI, it will address compliance in its wiretapping requirements document, which is being developed. The proposal also does not address the international implications of future technologies, such as PCN, on wiretapping. PCN will involve assigning a subscriber one telephone number. All calls will be billed to that number regardless of what instrument or network the subscriber uses. Using PCN, the subscriber may be anywhere in the world, and the service may be provided by any service provider using any technology. Since some of the service providers may be international, and since the providers may be outside the United States, the FBI will have to establish cooperative arrangements with foreign law enforcement agencies in order to wiretap.

In May 1992, the FBI formed a technical committee composed of staff from the FBI and the telecommunications industry. The purpose of this committee is to identify technological alternatives and select the alternatives that best meet the FBI's needs. As of June 1992, the committee was developing its charter. These FBI efforts are steps in the right direction.

Scope and Methodology

We identified and assessed the technological alternatives for wiretapping in the following technologies: (1) analog and digital using copper wire transport, (2) analog and digital using fiber optic transport, (3) ISDN, (4) PBX, (5) broadband, (6) cellular, (7) satellite, (8) PCS, and (9) PCN. As part of our assessment, we also analyzed the wiretapping implications of special features associated with these technologies, such as call forwarding and voice mail. On the basis of our analysis of the technologies and discussions with representatives of the telecommunications industry, we identified the six primary wiretapping locations.

We also assessed the FBI's past and current actions to satisfy its wiretapping needs, including its April 1992 proposal to amend the Communications Act of 1934, and its May 1992 proposal.

We met with the FBI's Assistant Director and Deputy Assistant Director (Operations), Technical Services Division, and technical managers from the FBI Engineering Research Facility to discuss the FBI's progress in defining and communicating its wiretapping needs. We also held technical discussions on the above technologies with four Bell operating telephone companies, two switch manufacturers, two cellular providers, two cellular and satellite manufacturers, and the associations of the International Chiefs of Police and Major Cities Chiefs of Police. In addition, we contacted the National Security Agency, which told us that it does not have expertise in these areas. We performed our work at FBI's headquarters office in Washington, D.C., and Engineering Research Facility in Quantico, Virginia, as well as at the corporate offices of the industry representatives visited in various locations nationwide.

Our work was performed between April and June 1992 in accordance with generally accepted government auditing standards.

We did not obtain written comments on this report. However, we briefed FBI officials, including the Assistant Director and Deputy Assistant Director (Operations), Technical Services Division, on the results of our work and on our discussions with the telecommunications industry. These officials generally agreed with the facts as presented, including our technical assessment of the wiretapping alternatives. We have incorporated their views, as well as their updates on the FBI's planned actions, in the report as appropriate.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan to make no further distribution until 30 days from the date of this letter. We will then send copies to the Attorney General; the Director of the Federal Bureau of Investigation; the Director, Office of Management and Budget; and interested congressional committees. Copies will also be made available to others upon request. This report was prepared under the direction of Howard G. Rhile, Director, General Government Information Systems, who can be reached at (202) 512-6418. Major contributors to this report are listed in appendix II.

Sincerely yours,



for Ralph V. Carlone
Assistant Comptroller General



General Services Administration
Office of Congressional Affairs
Washington, DC 20405

9C12 (1)(b) -
File 1

#4

Control No: 92031208	
Due Date: 3-12-92 9:00 PM	
Signature of:	
Action Office: KAM	
Information:	
Copy to:	
Date Rec'd: 3/12/92	Time: 12:29 PM

DATE: March 12, 1992

FROM: Office of Congressional Affairs (S)

SUBJECT: Draft Bill No. 118 - Justice Draft Bill, Digital Telephony

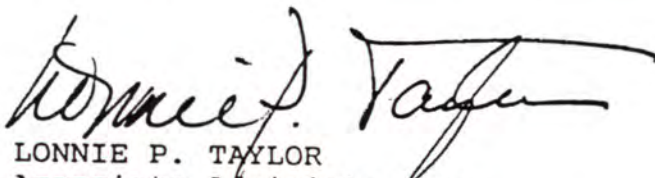
TO: L
T
K ✓
J
P

You are requested to prepare a memorandum stating your views and recommending an agency position on the attached bill. In the event your office has no interest in the subject matter of the bill, please submit a negative reply.

The memorandum is due in the Office of Congressional Affairs (S) by C.O.B., Today.

Please complete the memorandum in sufficient time to allow for adequate review by the appropriate division of the Office of General Counsel prior to submission to S. If the deadline cannot be met, S must be contacted prior to the due date to arrange for an extension. S will assume that, in absence of a request for an extension, the failure to meet a deadline means that the service has no comment.

If you have any questions, please call me or Brenda Robinson on 501-0563.


LONNIE P. TAYLOR
Associate Administrator
for Congressional Affairs

cc: M
LaFlam
Piper

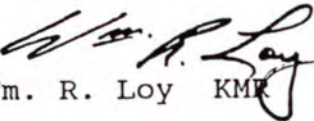
(#4)

Control No. X92031208
Due Date: 3/12/92 COB
Ext. Due Date: 3/13/92 9AM

Brenda Robinson (S)

After KMR consultations, we "cannot support" Draft Bill No. 118 as currently drafted for the reasons stated in our attachment.

If OMB later allows sufficient time for a more thorough review and response, our comments will be provided in a formal format.


Wm. R. Loy KMR 3/13/92 9AM

Attachment

Info: K(Peay), KD, KA, KB, KE, KG, KV, ^{KM,} KMP, KMR, R/F, LP-Rm. 4002

O/F - 9C1h(1)(a) - File 2 (#4)

ATTACHMENT

The proposed legislation could have a widespread impact on the government's ability to acquire new telecommunications equipment and provide electronic communications services.

Existing Federal government telecommunications resources may be affected by the proposed new technology techniques and equipment. An incompatibility and interoperability of existing Federal government telecommunications systems and resources could result due to the new technological changes proposed.

The Federal Communications Commission's implementation of the proposed modifications to the "Communications Act of 1934" could also cause an unknown effect on the communications systems operations, services, equipment, and regulations within the Federal government. Further, to change the entire United States telecommunications infrastructure in the proposed 180 days seems very optimistic, no matter how trivial the proposed modifications are to implement.

Finally, there would be unknown associated costs to implement the proposed new technological procedures and equipment. These costs would be borne by the Federal government, consumers, and all other communications ratepayers to finance the effort. Both the Federal government and private industry communications regular phone service, data transmissions, satellite and microwave transmissions, and encrypted communications could be effected at increased costs.



General Services Administration
Office of Congressional Affairs
Washington, DC 20405

13RUCF

WANDA IRMS-K 3:55	
Control No: X92050405	
Due Date: 5-5-92	
Signature of:	
Action Office: KMR	
Information:	
Copy to:	
Date Rec'd Of	Time
5-1-92	3:51

9-1-92 (2)(a) File #4A

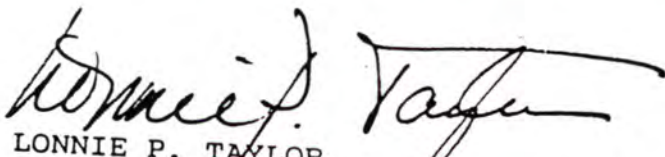
DATE: May 1, 1992
FROM: Office of Congressional Affairs (S)
SUBJECT: Revised Draft Bill No. 118
TO: L
P
(K)
T
J

You are requested to prepare a memorandum stating your views and recommending an agency position on the attached bill. In the event your office has no interest in the subject matter of the bill, please submit a negative reply.

The memorandum is due in the Office of Congressional Affairs (S) by May 5, 1992.

Please complete the memorandum in sufficient time to allow for adequate review by the appropriate division of the Office of General Counsel prior to submission to S. If the deadline cannot be met, S must be contacted prior to the due date to arrange for an extension. S will assume that, in absence of a request for an extension, the failure to meet a deadline means that the service has no comment.

If you have any questions, please call me or Brenda Robinson on 501-0563.


LONNIE P. TAYLOR
Associate Administrator
for Congressional Affairs

cc: M
Piper
I Flam

#4A

Control No. X92050405

Due Date: 5/5/92

Brenda Robinson (S)

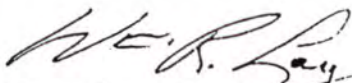
After KMR consultations, we still "cannot support" Draft Bill No. 118 as substantially revised by Justice after its purported full consideration of other agencies' "substantive concerns."

Aside from the third paragraph of our 3/13/92 attachment response for the original draft bill, which was adopted as GSA's position (copy attached), Justice has failed to fully address other major GSA concerns (i.e., technological changes and associated costs).

Further, by merely eliminating the FCC and any discussion of cost issues in the revision, we can not agree as contended by Justice that it now "...takes care of the kinds of problems raised by FCC and others...."

Finally, the revision gives Justice sole unilateral exclusive authority to enforce and except or waive the provisions of any resultant law in Federal District Courts. Our other concerns are also shown in the current attachment for the revised draft bill.

Once again OMB has not allowed sufficient time for a more thorough review, a comprehensive internal staffing, or a formal response.



Wm. R. Loy KMR 5/5/92

Info: K(Peay), KD, KA, KB, KE, KG, KV, KM, KMP, KMR, R/F, LP-Rm. 4002

(O/F) - 9C1h(Z) (A) - File (#4A)

ATTACHMENT
REVISED JUSTICE DRAFT BILL
DIGITAL TELEPHONY

The proposed legislation could have a widespread impact on the government's ability to acquire new telecommunications equipment and provide electronic communications services.

Existing Federal government telecommunications resources will be affected by the proposed new technology techniques and equipment. An incompatibility and interoperability of existing Federal government telecommunications systems and resources would result due to the new technological changes proposed.

The Federal Communications Commission (FCC) has been removed from the legislation, but the Justice implementation may require modifications to the "Communications Act of 1934" and other FCC policies and regulations to remove inconsistencies. This could also cause an unknown effect on the wire and electronic communications systems operations, services, equipment, and regulations within the Federal government. Further, to change a major portion of the United States telecommunications infrastructure (the public switched network within eighteen months and others within three years) seems very optimistic, no matter how trivial or minimal the proposed modifications are to implement.

In the proposed legislation the Attorney General has sole unilateral exclusive authority to enforce, grant exceptions or waive the provisions of any resultant law and enforce it in Federal District Courts. The Attorney General would, as appropriate, only "consult" with the FCC, Department of Commerce, or Small Business Administration. The Attorney General has exclusive authority in Section 2 of the legislation; it appears the Attorney General has taken over several FCC functions and placed the FCC in a mere consulting capacity.

The proposed legislation would apply to all forms of wire and electronic communications to include computer data bases, facsimile, imagery etc., as well as voice transmissions.

The proposed legislation would assist eavesdropping by law enforcement, but it would also apply to users who acquire the new technology capability and make it easier for criminals, terrorists, foreign intelligence (spies) and computer hackers to electronically penetrate the phone network and pry into areas previously not open to snooping. This situation of easier access due to new technology changes could therefore affect national security.

The proposed legislation does not address standards and specifications for telecommunications equipment nor security considerations. These issues must be addressed as they effect both the government and private industry. There are also civil liberty implications and the public's constitutional rights to privacy which are not mentioned.

It must be noted that equipment already exists that can be used to wiretap the digital communications lines and support court-authorized wiretaps, criminal investigations and probes of voice communications. The total number of interception applications authorized within the United States (Federal and State) has been averaging under nine hundred per year. There is concern that the proposed changes are not cost effective and worth the effort to revamp all the existing and new telecommunications systems.

The proposed bill would have to have the FCC or another agency approve or reject new telephone equipment mainly on the basis of whether the FBI has the capability to wiretap it. The federal approval process is normally lengthy and the United States may not be able to keep pace with foreign industries to develop new technology and install secure communications. As a matter of interest, the proposed restrictive new technology could impede the United States' ability to compete in digital telephony and participate in the international trade arena.

Finally, there will be unknown associated costs to implement the proposed new technological procedures and equipment. These costs would be borne by the Federal government, consumers, and all other communications ratepayers to finance the effort. Both the Federal government and private industry communications regular phone service, data transmissions, satellite and microwave transmissions, and encrypted communications could be effected at increased costs.

Return to O/F

#4B

(Control No. - N/A)
Due Date: 5/20/92

Brenda Robinson (S)

After KM consultations, and considering the lack of (L) or (T) supporting comments, we elect not to pursue an appeal of OMB's 5/19 decision to override our comments which represented GSA's position on the Justice Revised Draft Bill No. 118 concerning digital telephony.



Wm. R. Loy KMR 5/20/92

Info: K(Peay), KD, KA, KB(2), KG(2), KV(2), KM, KMP, KMR, R/F, LP-Rm. 4002

O/F - 9C1h(1)(b) - File 1 (#4B)

[Consensus decision of KB (Lai), KG (Culberson), KM (Sims), and KV (Edwards) based on K's isolated GSA opposition to OMB. WRL]

F.B.I.'s Proposal on Wiretaps Draws Criticism From G.S.A.

By ANTHONY RAMIREZ

Nine months after the Federal Bureau of Investigation proposed a law to make the nation's telephones easier to wiretap, the legislative proposal has yet to find a Congressional sponsor. One reason may be division within the Government over the wisdom of the proposal, according to newly released documents detailing unusually sharp criticism of the F.B.I. by the General Services Administration.

In the documents, the G.S.A. said the proposed legislation was unnecessary, could hurt the nation's competitiveness in "the international trade arena" and posed a possible danger to national security.

The F.B.I. plan is one of the thornier issues confronting the incoming Clinton Administration and the Attorney General-designate, Zoë Baird. No senator or representative has introduced the legislation, first proposed in March, but the F.B.I. expects a legislator to introduce it by spring.

The issue centers on digital transmission and fiber-optic cables and how they make it more difficult for the F.B.I. to wiretap the calls of mobsters, terrorists and other criminals.

Passing On the Costs

The F.B.I. proposal would require the licensing of millions of dollars of telephone equipment by the Government so the agency could wiretap it. The cost of any change, for which there are no estimates, would be passed on to customers. Civil liberties groups, joined by some phone companies, including A.T.&T., call the plan an invasion of privacy.

The General Services Administration documents, dated May 1992, were obtained by a Washington group through a legally enforceable request under the Freedom of Information Act. The group, Computer Professionals for Social Responsibility, opposes the F.B.I. legislation and provided the documents to The New York Times. Margaret Truntich, the G.S.A. official whose division prepared the documents, confirmed their authenticity.

An F.B.I. official said earlier this week that the G.S.A. memo was ill informed and out of date. "Basically, G.S.A. just didn't understand what was going on," said Barry Smith, a special agent in the F.B.I.'s Office of Congressional Affairs.

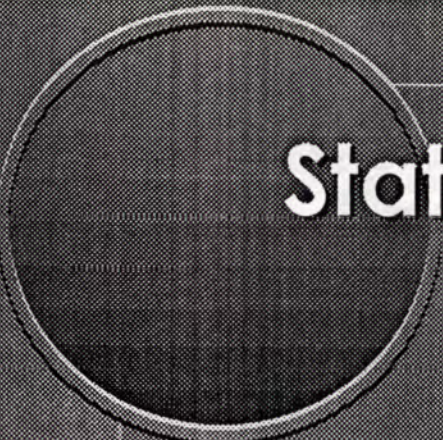
One G.S.A. memo criticized the F.B.I. proposal for seeking the revamping of the nation's phone system when "equipment already exists that can be used to wiretap the digital communications lines."

Remote Wiretaps

The F.B.I. proposal would also require phone companies to make it possible to wiretap calls from remote sites, rather than, as today, tapping into phone lines directly outside, say, a mobster's house.

Such changes, the G.S.A. said, would "make it easier for criminals, terrorists, foreign intelligence and computer hackers to electronically penetrate the phone network and pry into areas previously not open to snooping" by using the same remote techniques.

In the standard analog transmission, variations in electrical voltage imitate the sound of a human voice. But phone systems are being rapidly converted to high-capacity digital lines in which the human voice is converted into numbers. Fiber-optic lines use pulses of light.



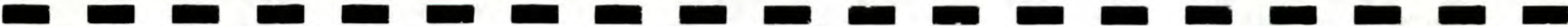
Statistical Analysis of Electronic Surveillance

National Institute of Standards and Technology,
Computer System Security and Privacy
Advisory Board
June 3, 1993

David Banisar
CPSR Washington Office
Banisar@washofc.cpsr.org

CPSR 1993





Wiretap in Practice

- Very Small (VS) number of lawful wiretaps in the US
- Wiretap is involved in VS percentage of all arrests
- Primarily for narcotics offenses(70 percent in 1992)

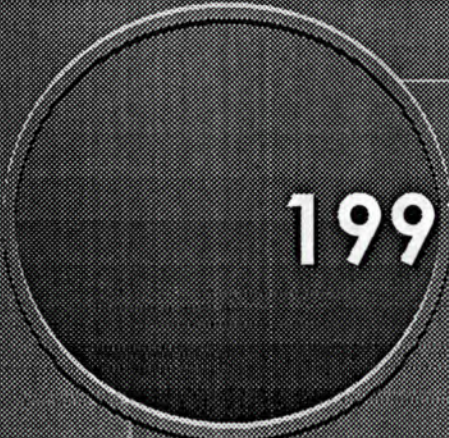
CPSR 1993

Wiretap Trends, 1968-1992

- Cost of wire surveillance has increased
- Number of conversations intercepted has increased
- Number of non-incriminating conversations intercepted has increased
- Number of incriminating conversations intercepted has remained unchanged
- Arrests have remained unchanged

Source: Administrative Office of US Courts

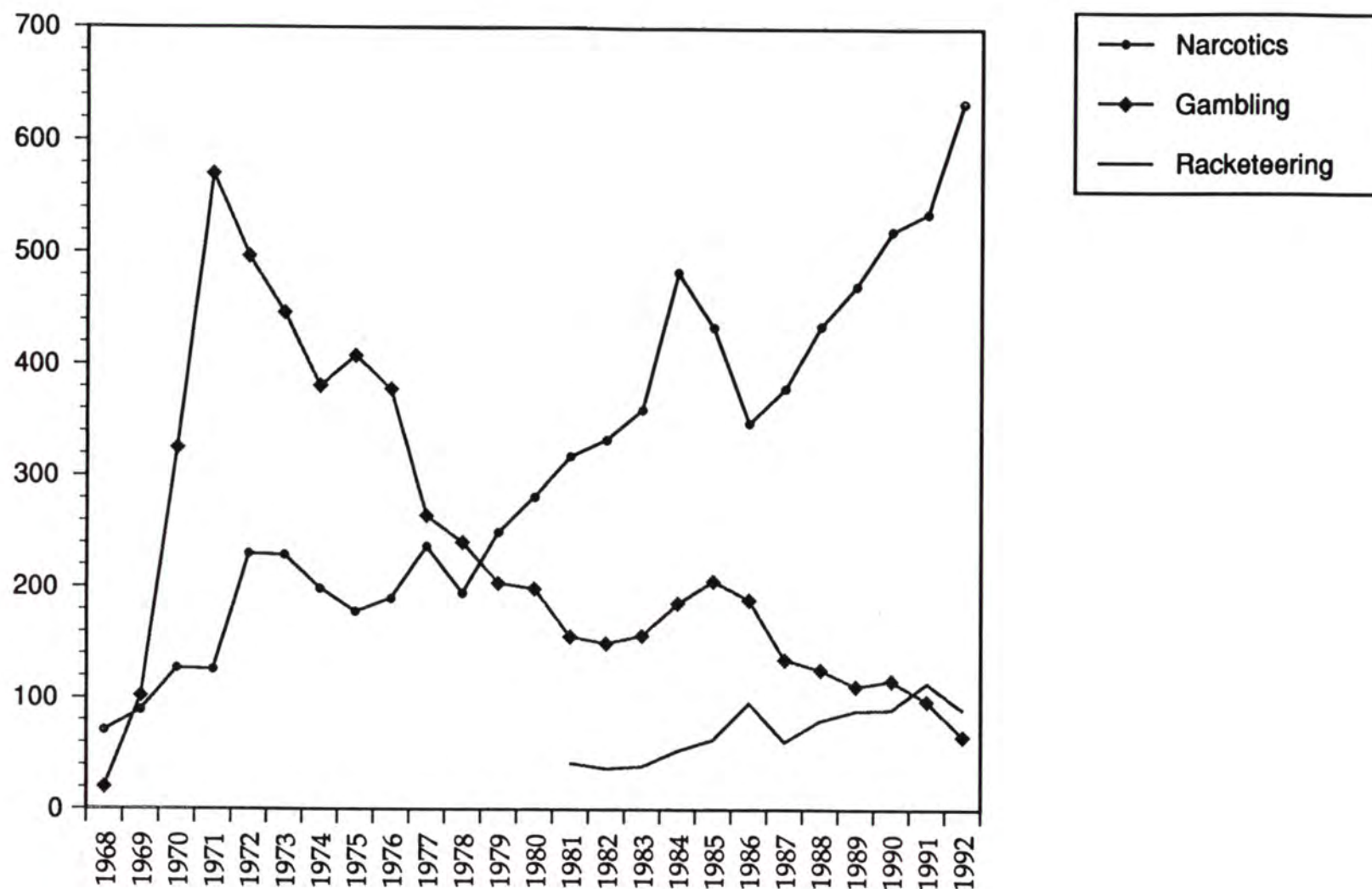
CPSR 1993



1991 Statistics

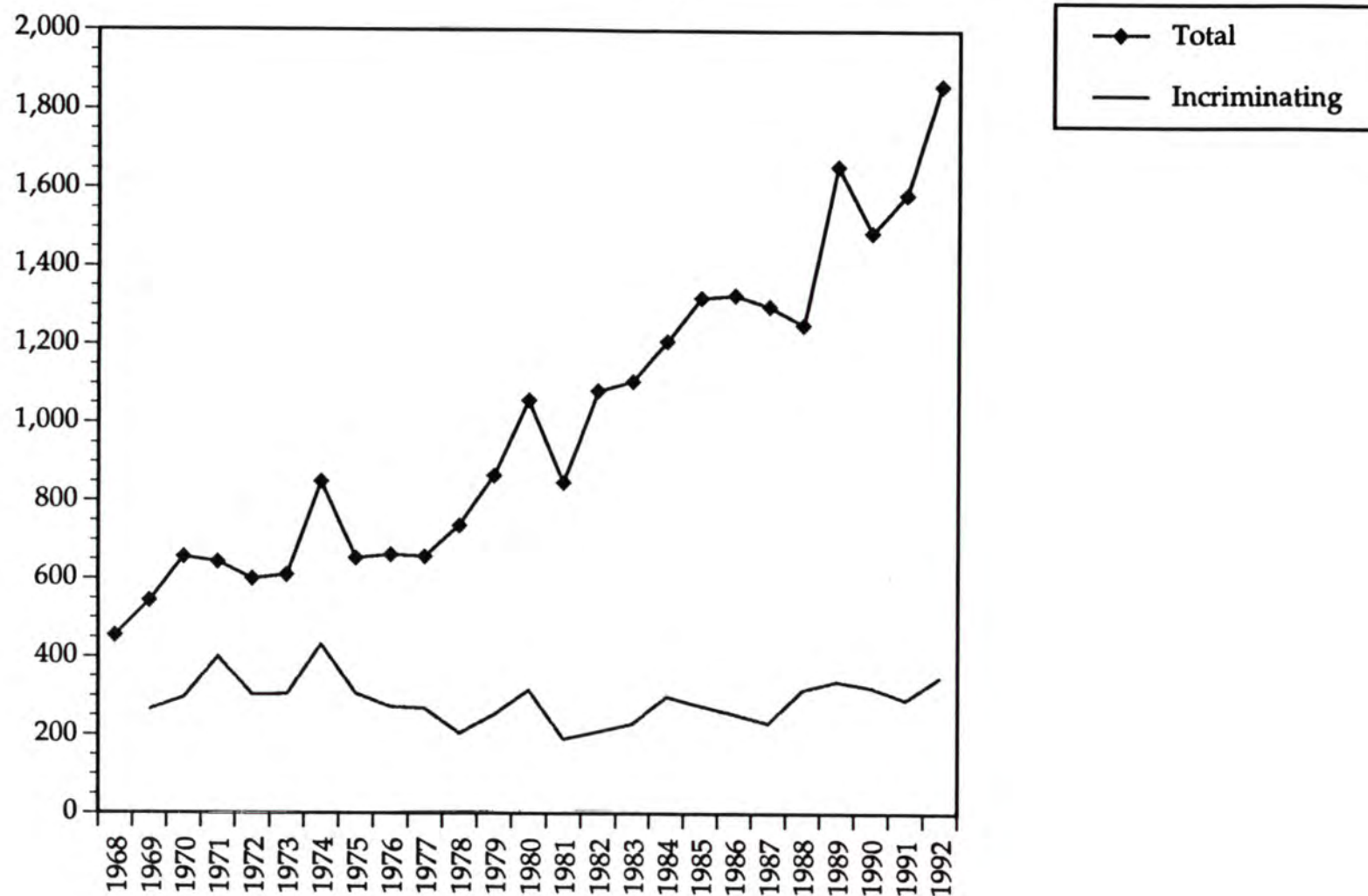
- 1/2 trillion phone calls placed
- 140 million phone lines in operation
- 856 Title III intercepts (includes taps, bugs and other techniques)
- 1.35 million conversations overheard
- 14 million total arrests in US
- 3,000 arrests as result of court authorized intercepts

Title III Intercepts by Offense 1968-1992



Source: Administrative Office of the US Courts

Total Conversations Overheard and Incriminating Conversations Overheard per Title III Intercept 1968-1992 (average)



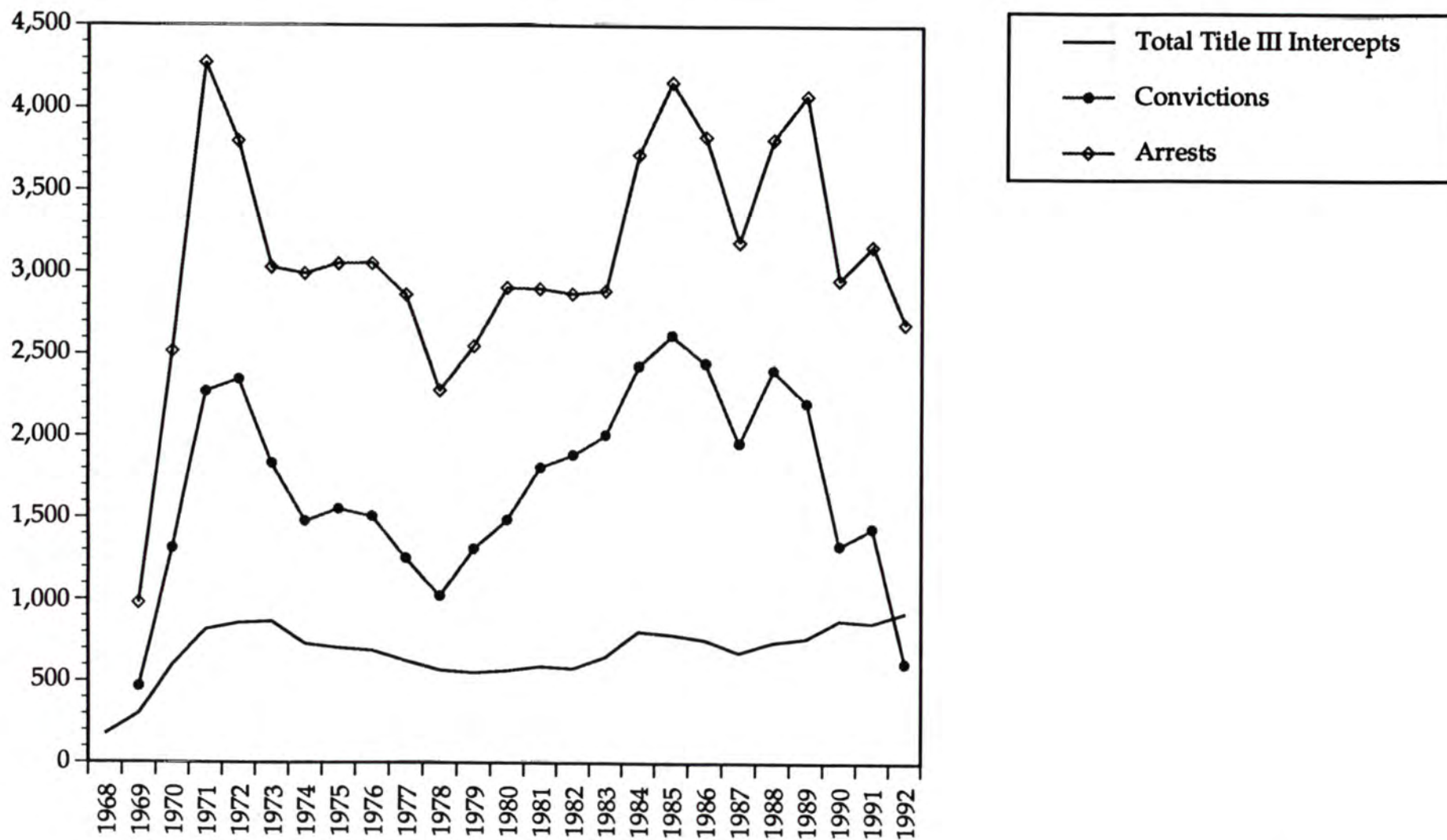
Source: Administrative Office of the US Courts

Estimated Total Number Individuals Overheard Each Year 1968-1992



Source: Administrative Office of the US Courts

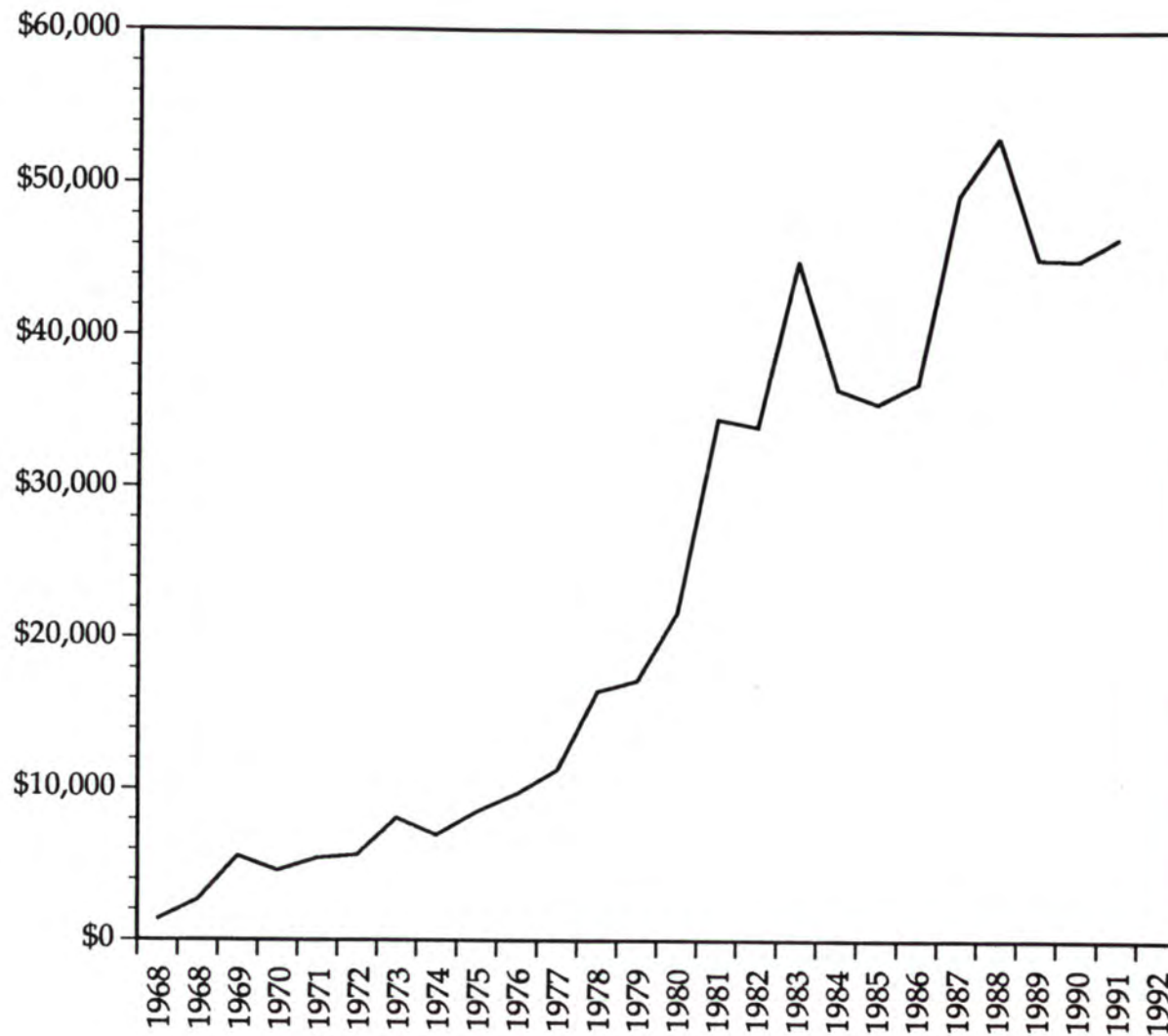
Title III Interceptions and Resulting Arrests and Convictions 1968-1992



Source: Administrative Office of the US Courts

CPSR 1993

Cost of Each Title III Intercept(Average) 1968-1992



Source: Administrative Office of the US Courts
Not Adjusted for Inflation

CAN WIRETAPS REMAIN COST-EFFECTIVE?

by Robin Hanson
hanson@ptolemy.arc.nasa.gov
510-651-7483
47164 Male Terrace, Fremont, CA 94539

May 12, 1993
Distribute Freely

SUMMARY: Compared to an average monthly phone bill of seventy dollars, the option to wiretap the average phone line is probably worth less than twelve cents a month to police and spy agencies. Claims that this option is worth over a dollar a month ignore the basic economics of law enforcement. Thus recently proposed government policies to preserve wiretap abilities in the face of technological change must raise phone costs by less than one part in seven hundred to be cost-effective. Why not let a market decide if wiretaps make sense?

BACKGROUND

Until now, telephones have happened to allow the existence of "wiretaps", cheap detectors which can pick up conversations on a phone line without the consent of either party to the conversation. And since 1968, U.S. police have been allowed to request such wiretaps from judges, and must compensate phone companies for expenses to assist a tap. Since then, law enforcement agencies have come to rely on this capability to aid in criminal investigations.

However, wiretaps have become more difficult as phone companies have switched to digital technologies. And powerful new encryption technologies threaten to make truly private communication possible; a small chip in each phone could soon make it virtually impossible to overhear a conversation without a physical microphone at either end. So the U.S. government has begun to actively respond to these threats to police wiretap abilities.

Regarding digital phone issues, a "FBI Digital Telephone Bill" was circulated early in 1992 [1], proposing to require all communication services to support easy wiretaps, now without compensation from the police. Each tapped conversation would have to be followed smoothly as the parties used call-forwarding or moved around with cellular phones. The data for that conversation would have to be separated out from other conversations, translated to a "form representing the content of the communication", and sent without detection or degradation to a remote government monitoring facility, to be received as quickly as the parties to the conversation hear themselves talk. Congress has yet to pass this bill.

Regarding encryption issues, the White House announced on April 16, 1993 that 1) they had developed and begun manufacturing a special "wiretap" (or "Clipper") chip to be placed in future phones, instead of the total privacy chips which have been under private development, 2) they plan to require this chip in most phones the government buys, and 3) they will request

all manufacturers of encrypted communications hardware to use this wiretap chip. The same day, AT&T announced it would use these chips "in all its secure telephone products".

The plan seems to be to, at the very least, create a defacto standard for encryption chips, so that alternatives become prohibitively expensive for ordinary phone users, and to intimidate through the threat of further legislation. Such legislation would be required to stop privacy fans and dedicated criminals, who might be willing to pay much more to use an alternative total privacy standard.

Both the specific wiretap chip design and the general algorithm are secret. Each chip would be created under strict government supervision, where it would be given a fixed identifier and encryption key [2]. At some unspecified frequency during each conversation, the chip would broadcast its identifier and other info in a special "law enforcement field". Law enforcement officers with a court order could then obtain the key corresponding to this identifier from certain unspecified agencies, and could thereby listen in on any future or previously recorded conversations on that phone.

To date, most concerns voiced about the wiretap chip have been about its security. Encryption algorithms are usually published, to allow the absence of public demonstrations of how to break the code to testify to the strength of that code. And it is not clear what government agency could be trusted with the keys. Many suspect the government will not limit its access in the way it has claimed; the track records of previous administrations [3], and of foreign governments [4], do not inspire confidence on this point.

This paper, however, will neglect these concerns, and ask instead whether this new wiretap chip, and other policies to preserve phone wiretaps, are cost-effective tools for police investigation. That is, which is a cheaper way for society to investigate crime: force phone communications to support wiretaps, or give police agencies more money to investigate crimes as they see fit? Or to put it another way, would police agencies still be willing to pay for each wiretap, if each wiretapping agency were charged its share of the full cost, to phone users, of forcing phones to support wiretaps?

A recent U.S. General Accounting Office report on the FBI bill stated [1]:

"[N]either the FBI nor the telecommunications industry has systematically identified the alternatives, or evaluated their costs, benefits, or feasibility."

While this paper will not change this sad fact, it does aspire to improve on the current confusion. To begin to answer the above questions, we might compare the current benefits wiretaps provide to law enforcement agencies with projected costs of implementing the new wiretap chip and other wiretap policies.

WIRETAP BENEFITS

1990 is the latest year for which wiretap statistics are widely available [5], though wiretap activity has been rather steady in recent years. According to the Office of U.S. Courts, 872

wiretap installations were requested by local, state, and federal police in 1990, and no requests were denied. 2057 arrests resulted from wiretaps started the same year, 1486 arrests came from wiretaps in the previous ten years, and 55% of arrests led to convictions. About 40% of wiretaps were requested by federal authorities, while several states, including California and Illinois, still do not allow wiretaps. About 60% of taps were regarding drug offenses, and 14% for gambling offenses. Wiretaps are most useful for investigating "victimless" crimes, since victims will often give police permission to record their calls.

Each wiretap installation heard an average of 1487 calls, 22% of them incriminating, among 131 people, and cost an average of \$45,125, mostly for labor (extrapolating from the 91% of installations reporting costs). \$1.6 million was also spent following up on wiretaps from previous years. Thus a total of about \$41 million was spent on wiretaps, to obtain about 4000 arrests, at about \$10,000 per arrest, or four times as much as the \$2500 per arrest figure one gets by dividing the \$28 billion spent by all police nationally by the total 11 million non-traffic arrests [6]. Thus wiretaps are a relatively expensive form of investigations.

76% of the wiretaps were for phone lines (vs pagers, email, etc.), and are the focus of this paper. The \$31 million per year spent on phone taps represents only one thousandth of the total police expenditures, and if we divide this by the 138 million phone "access" lines in the country [6], we get about 23 cents spent per year per phone line, or about two cents a month. Since 1978, our foreign intelligence agencies have also been authorized to tap international phone calls. No statistics are published on these taps, so let us assume a similar number of "spy" wiretaps are done, giving a total of ~\$60 million annually, or four cents per month spent on wiretaps per phone line.

Of course the amount police spend on wiretaps is not the same as the benefits of wiretaps. How can we estimate benefits? Dorothy Denning, an advocate of both the FBI bill and the wiretap chip, claims that "the economic benefits [of wiretaps] alone are estimated to be billions of dollars per year" [7], and then refers to amounts fined, recovered, and "\$2 billion in prevented potential economic loss" by the FBI from 1985 to 1991. Denning further relays fascinating FBI claims that through wiretaps "the hierarchy of organized crime has been neutralized or destabilized", and that "the war on drugs ... would be substantially ... lost" without them.

Two billion dollars per year of wiretap benefit would translate to a little over a dollar a month per phone line. Denning, however, offers no support for her claims, and appears to be relaying internal FBI figures, which the FBI itself has neither revealed nor explained to the public. And the FBI is hardly a neutral party on this subject.

Estimating the benefits of police investigations is not as simple as it might seem, however, and certainly requires more than adding up amounts fined or recovered. Long and well-established results in the economics of law enforcement [8] tell us to reject the notion that we should be willing to spend up to one dollar on police, in order to collect another dollar in fines or to prevent another dollar of theft. So, for example, we rightly reject IRS pleas for increased budget based solely on estimates of how many more dollars can be collected in taxes for each dollar spent by the IRS. In fact, a main reason given for using public police to investigate crime, instead of private bounty hunters, is to avoid such police overspending.

In general, we deter a given class of criminals through a combination of some perceived probability of being caught and convicted, and some expected punishment level if convicted. And some crime is directly prevented, rather than deterred, through some level of police monitoring. The optimum police budget is a complex tradeoff between social costs due to the crimes themselves, the punishment exacted, and police expenses.

How then can we estimate wiretap benefits? Let us assume that about the right total amount is being spent on police, and that police have about the right incentives, to spend their budget to monitor where it would help the most, and to get as many as possible of the right kinds of convictions. (If police budgets are too low, then the answer is to increase them, rather than trying to crudely subsidize any one of their expenses.)

In this case the social benefit of being able to wiretap is no more than about the additional amount police would be willing to pay, beyond what they now pay, to undertake the same wiretaps (assuming this remains a small fraction of total police budgets). The benefit of wiretaps is actually less than this value, because were wiretaps to become more expensive, we might prefer to get the same criminal deterrence by instead raising punishment and lowering the probability of conviction, or perhaps we might accept a lower deterrence level, or even decriminalize certain activities. Police monitoring might be similarly adjusted.

How much police would be willing to pay for each wiretap would depend of course on how what alternatives are available. If unable to wiretap a particular suspect's phone line, police might instead use hidden microphones, informants, grant immunity to related suspects, or investigate a suspect in other ways.

The law requires that police requesting a wiretap must convince a judge that other approaches "reasonably appear to be unlikely to succeed if tried or to be too dangerous". But in practice judges don't often question boilerplate claims to this effect in police requests [9], and investigations often continue even after a wiretap has failed to aid an investigation. Experienced investigators advise wiretaps as a last resort, but mainly because wiretaps are so expensive.

More importantly, police can also choose to focus on similar suspects who are more easily investigated without wiretaps. Most police cases are near the borderline where it is not clear that they are worth pursuing, and will be simply dropped should a more pressing case suddenly arise. Many cases reach the point where a wiretap might help, but are dropped because a wiretap seems too costly. And most cases now using wiretaps would probably be abandoned if wiretaps became dramatically more expensive.

No doubt a few wiretaps are so valuable that it would have cost ten times as much to obtain similar results through other means. But on average, it is hard to imagine that police would be willing to pay more than a few times what they now pay for each wiretap. If we assume that police would on average be willing to pay twice as much for each tap, then the social benefit of phone wiretaps is about equal to the current spending level of four cents a month per phone line.

If we assume that police would on average be willing to pay four times as much per wiretap, the option to wiretap the average phone would be worth twelve cents a month.

A better estimate of wiretap values might come from randomly asking recent wiretap requestors whether they would have still requested that wiretap had they expected it to take twice as much labor to get the results they had expected, or three times as much, etc. The FBI will not allow such a survey by ordinary citizens, but perhaps some state police would. But until such research is done, the twelve cent figure seems a reasonably generous estimate, and the four cent figure may be closer to reality,

Of course the value of the option to tap any particular phone line presumably varies a great deal from the average value. But unless the police can somehow pay only for the option to wiretap particular phone lines of its choosing, it is the average value that matters for a cost/benefit analysis.

WIRETAP COSTS

Let us for the moment optimistically assume that the U.S. government encryption scheme used in the wiretap chip is as secure as whatever private enterprise would have offered instead, protecting our conversations from the spying ears of neighbors, corporations, and governments, both foreign and domestic. Even so, the use of this chip, and of other policies to support wiretaps, would create many additional costs to build and maintain our communication system.

Some phone companies must have perceived a non-trivial cost in continuing to support wiretaps while moving to digital phone transmissions, even when compared to the widely recognized value of staying on the good side of the police. Otherwise the police would not have complained of "instances in which court orders authorizing the interception of communications have not been fulfilled because of technical limitations within particular telecommunications networks" [1].

The wiretap chip requires extra law enforcement fields to be added to phone transmissions, increasing traffic by some unknown percentage. A special secure process must be used to add encryption keys to chips, while securely distributing these keys to special agencies, which must be funded and monitored. The chips themselves are manufactured through a special process so that the chip becomes nearly impossible to take apart, and the pool of those who can compete to design better implementations is severely limited. Private encryption systems not supporting wiretaps would require none of these extra costs.

Perhaps most important, government decree would at least partially replace private marketplace evolution of standards for how voice is to be represented, encrypted, and exchanged in our future phones. It is widely believed that governments are less efficient than private enterprise in procuring products and standards, though they may perhaps perform a useful brokering role when we choose between competing private standards. How much less efficient is a matter of debate, some say they pay twice as much, while others might say they pay only 10% more.

This type of wiretap support also raises costs by preventing full use of a global market for telephone systems. It pushes certain domestic phone standards, which foreign countries may not adopt, and requires the use of encryption methods known only to our government, which foreign countries are quite unlikely to adopt.

In 1990, 53 U.S. phone companies had total revenues of \$117.7 billion for domestic calls, \$4.4 billion for overseas calls, and \$4.5 billion for cellular calls [6], for a total cost of \$126.6 billion dollars to run the phone system, and an average monthly phone bill of \$76.45 per line. If we generously assume that police and spies would on average be willing to pay four times as much as the ~\$60 million they now spent on wiretaps annually, we find that wiretaps are not cost effective if we must raise phone costs by as much as one part in 700 to preserve wiretap abilities in the face of technological change. The twelve cents per line wiretap option value must be compared with an average seventy dollar monthly phone bill. (If we assume that police would only pay twice as much on average, then this limit falls to one part in 2000!)

Dorothy Denning relays FBI claims that \$300 million is the maximum cumulative development cost "for a switch-based software solution" so that phone companies can continue to support wiretaps [7]. Denning does not, however, say how long this solution would be good for, nor what the software maintenance and extra operating costs would be. And again this is a figure which the FBI itself has neither revealed nor explained to the public. If we use a standard estimate that software maintenance typically costs twice as much as development [10], and accept this FBI estimate, then this extra software cost would be by itself five times the above generous estimate of annual wiretap benefits.

The current government contractor claims it will offer the wiretap chips for about \$26 each in lots of 10,000 [2], over twice the \$10 each a competing private developer claims it would charge [11] for a chip with comparable functionality, minus wiretap support. And the wiretap chip price probably doesn't reflect the full cost of government funded NSA research to develop it. If only one phone (or answering machine) is replaced per phone line every five years, the extra cost for these chips alone comes out to over 27 cents extra a month per line, or by itself more than two times a twelve cent estimated wiretap option value. Of course most phones wouldn't have encryption chips for a while, but the wiretap benefit is per phone, so this argument still applies.

COMPARING BENEFITS AND COSTS

Given the dramatic difference between the total cost of running the phone system and an estimated social value of wiretaps, we can justify only the slightest modification of the phone system to accommodate wiretaps. When the only modification required was to allow investigators in to attach clips to phone wires, wiretap support may have been reasonable. But when considering more substantial modification, the burden of proof is clearly on those proposing such modification to show how the costs would really be less than the benefits. This is especially true if we consider the costs neglected above, of invasions of the privacy of innocents, and the risk that future administrations will not act in good faith [3].

If consensus cannot be obtained on the relative costs and benefits of wiretaps, we might do better to focus on structuring incentives so that people will want to make the right choices, whatever those might be. Regarding phone company support for wiretaps, it seems clear that if wiretaps are in fact cost-effective, there must be some price per wiretap so that police would be willing to pay for wiretaps, and phone companies would be willing to support them. As long as the current law requiring police to pay phone company "expenses" is interpreted liberally enough, the market should provide wiretaps, if they are valuable.

Monopoly market power of phone companies, or of police, might be an issue, but if we must legislate to deal with monopoly here, why not do so the same way we deal with monopoly elsewhere, such as through price regulation? Legislating the price to be zero, however, as the FBI bill seems to propose, seems hard to justify. And having each police agency pay for wiretaps, rather than all phone companies, seems fairer to states, such as California and Illinois, which do not allow wiretaps.

Regarding encryption chips, recall that without legislation outlawing private encryption, serious criminals would not be affected. In this case, it does not seem unreasonable to allow phone companies to offer discounts to their customers who buy phones supporting wiretaps, and thereby help that phone company sell wiretaps to police. Each phone user could then decide if this discount was worth buying a more expensive phone chip, and risking possible unlawful invasions of their privacy. Adverse selection, however, might make privacy lovers pay more than they would in an ideal world.

If outlawing private encryption is seriously considered, then we might do better to instead just declare an extra punishment for crimes committed with the aid of strong encryption, similar to current extra punishments for using a gun, crossing state lines, or conspiring with several other people. As in these other situations, a higher punishment compensates for lower probabilities of convicting such crimes, and for higher enforcement costs, while still allowing individual tradeoffs regarding wiretap support.

If, as seems quite possible, the stringent cost requirements described here for preserving wiretap abilities cannot be met, then we should accept that history has passed the economical wiretap by. Police functioned before 1968, and would function again after wiretaps.

[1] <ftp://ftp.eff.org/pub/EFF/legislation/new-fbi-wiretap-bill> /[pub/EFF/legal-issues/eff-fbi-analysis](ftp://ftp.eff.org/pub/EFF/legal-issues/eff-fbi-analysis)

[2] Clipper Chip Technology, <ftp://csrc.ncsl.nist.gov/pub/nistnews/clip.txt>

[3] Alexander Charns, *Cloak and Gavel, FBI Wiretaps, Bugs, Informers, and the Supreme Court*, Univ. Ill. Press, Chicago, 1992.

[4] Headrick, *The Invisible Weapon*, Oxford Univ. Press, 1991.

[5] Report on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications, 1990, Administrative Office of U.S. Courts, Washington, DC 20544.

[6] Statistical Abstract of the United States, 1992.

[7] Dorothy Denning, "To Tap Or Not To Tap", Comm. of the ACM, March 1993.

[8] Richard Posner, Economic Analysis of Law, 4th Ed., 1992, Chapter 22.

[9] Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, Washington, 1976.

[10] Barry Boehm, Software Engineering Economics, Prentice Hall, 1981.

[11] conversation with Steven Bryen, representative of Secure Communications Technology, 301-588-2200, April 25, 1993.

No one paid Robin anything to write or research this (unfortunately :-)

=====



SOURCEBOOK
SOURCEBOOK
SOURCEBOOK
SOURCEBOOK
OF CRIMINAL JUSTICE STATISTICS — 1990
SOURCEBOOK
SOURCEBOOK
SOURCEBOOK
SOURCEBOOK
SOURCEBOOK
SOURCEBOOK

Table 2.49

Attitudes toward wiretapping

By demographic characteristics, United States, selected years 1974-90^a

Question: "Everything considered, would you say that you approve or disapprove of wiretapping?"

	1974			1975			1977			1978			1982			1983		
	Ap- prove	Disap- prove	No opinion	Ap- prove	Disap- prove	No opinion	Ap- prove	Disap- prove	No opinion	Ap- prove	Disap- prove	No opinion	Ap- prove	Disap- prove	No opinion	Ap- prove	Disap- prove	No opinion
National	16 %	80 %	4 %	16 %	80 %	4 %	18 %	78 %	3 %	19 %	78 %	3 %	19 %	77 %	4 %	18 %	78 %	4 %
Sex																		
Male	21	76	3	22	74	4	23	75	2	26	71	3	27	70	3	24	74	2
Female	13	83	5	12	84	4	14	82	4	14	83	3	14	82	4	15	80	5
Race																		
White	18	78	4	17	79	4	20	78	3	20	77	3	21	75	4	20	77	3
Black/other	7	90	3	11	84	5	10	85	5	8	88	3	7	89	4	8	84	9
Education																		
College	20	78	3	23	75	2	21	77	2	21	76	3	23	75	2	21	77	3
High school	16	80	3	14	82	4	19	78	3	19	79	2	18	78	3	17	79	4
Grade school	10	82	8	12	80	8	13	83	4	17	78	6	13	78	10	17	75	9
Occupation																		
Professional/business	19	78	2	23	75	2	24	74	2	22	74	3	24	74	2	22	75	3
Clerical	17	79	4	13	85	2	17	79	4	15	83	2	17	80	2	16	80	3
Manual	16	80	3	15	80	5	17	79	4	20	78	2	19	78	4	17	79	4
Farmer	10	83	7	13	80	7	17	80	3	8	84	8	31	54	15	20	72	8
Income																		
\$15,000 and over	22	77	2	17	81	2	23	75	2	21	77	2	23	74	3	21	77	2
\$10,000 to \$14,999	17	78	4	20	78	2	16	82	3	20	77	3	15	83	2	16	83	1
\$7,000 to \$9,999	14	84	2	17	78	5	16	82	3	16	79	3	14	83	3	14	80	6
\$5,000 to \$6,999	10	86	4	10	86	4	20	78	2	19	77	4	17	77	6	19	74	7
\$3,000 to \$4,999	17	80	3	13	80	6	15	82	3	18	80	2	15	78	6	7	89	4
Under \$3,000	8	84	8	14	81	5	10	86	4	11	84	4	10	84	5	16	76	8
Age																		
18 to 20 years	11	86	4	9	88	4	6	91	3	10	90	0	8	89	4	13	84	2
21 to 29 years	15	82	3	16	83	1	13	86	1	15	83	2	17	82	2	17	80	3
30 to 49 years	18	79	2	18	78	4	18	79	3	20	78	2	21	76	3	17	80	3
50 years and older	17	78	6	16	78	6	23	72	5	21	73	5	21	74	5	22	74	5
Region																		
Northeast	18	79	3	18	78	4	21	77	2	25	73	2	22	75	3	18	76	6
Midwest	14	82	4	17	80	3	22	76	2	16	83	2	18	80	2	19	78	3
South	16	80	4	15	80	4	14	82	4	19	77	4	17	78	5	18	78	4
West	20	77	3	14	81	5	19	78	3	17	78	4	23	73	4	19	78	3
Religion																		
Protestant	18	78	4	17	78	5	18	79	3	19	78	3	20	76	4	20	76	4
Catholic	15	82	4	15	83	2	20	77	3	18	79	2	17	80	3	18	77	4
Jewish	11	84	4	13	78	9	20	74	6	14	79	7	27	68	5	12	84	5
None	13	81	6	13	85	2	15	80	5	19	78	3	17	81	2	13	84	3
Politics																		
Republican	22	74	4	22	74	4	26	71	3	26	71	3	27	68	5	28	70	3
Democrat	13	84	3	12	85	3	17	81	2	16	81	3	16	80	4	15	82	4
Independent	18	79	4	18	78	5	16	80	4	18	79	3	18	79	3	16	78	5

Note: For a discussion of public opinion survey sampling procedures, see Appendix 5.

^aPercents may not add to 100 due to rounding.

Source: Table constructed by SOURCEBOOK staff from data provided by the National Opinion Research Center; data were made available through the Roper Public Opinion Research Center.

1985			1986			1988			1989			1990		
Ap- prove	Disap- prove	No opinion	Ap- prove	Disap- prove	No opinion	Ap- prove	Disap- prove	No opinion	Ap- prove	Disap- prove	No opinion	Ap- prove	Disap- prove	No opinion
23 %	74 %	3 %	22 %	74 %	4 %	20 %	74 %	6 %	26 %	69 %	5 %	22 %	72 %	6 %
30 17	66 80	3 3	26 19	71 76	2 5	26 16	69 78	5 7	32 22	64 73	4 5	24 20	71 73	5 6
25 10	73 84	3 7	24 10	72 85	3 5	21 16	73 79	6 4	29 11	66 85	5 4	24 13	71 77	5 9
25 22 18	73 74 77	2 4 5	24 22 20	73 75 73	3 3 7	20 20 23	75 75 63	4 5 14	27 28 16	69 68 73	4 4 11	22 23 19	74 71 68	4 7 13
27 21 21 22	71 76 75 78	2 3 4 0	25 21 20 29	72 75 76 71	3 4 3 0	24 19 18 14	72 74 76 79	4 7 6 7	30 24 24 8	65 72 72 77	5 4 5 15	25 19 22 21	70 78 72 68	5 3 6 10
25 25 10 27 14 15	73 73 88 67 81 80	2 2 2 6 5 5	25 19 9 17 21 22	72 78 85 79 72 73	2 3 7 4 7 5	22 19 15 17 19 17	74 78 74 73 68 77	4 3 11 10 13 7	28 23 22 28 13 20	69 73 70 63 81 70	3 4 8 9 6 10	24 18 26 16 16 17	73 75 72 76 71 67	3 7 2 8 13 17
16 19 24 24	80 79 73 73	4 2 3 3	16 18 22 25	84 79 76 69	0 2 2 6	21 15 21 22	76 79 75 69	3 6 4 8	38 30 23 28	62 64 74 66	0 6 3 6	38 23 19 24	62 73 76 68	0 4 5 8
26 22 22 24	70 75 75 75	4 4 3 1	22 23 22 22	74 74 74 74	4 3 4 3	23 20 19 21	73 74 75 73	4 6 6 6	27 30 24 25	65 66 72 71	8 4 4 4	21 27 20 18	74 68 72 77	5 5 8 5
23 23 23 21	74 74 74 77	3 3 3 2	22 24 21 19	74 73 76 77	4 3 3 4	22 20 15 10	72 74 80 82	5 6 5 8	27 26 17 28	69 69 75 67	4 6 8 5	26 16 25 18	68 80 70 73	6 5 5 9
24 21 24	73 77 72	2 2 4	25 21 22	70 76 75	5 3 3	29 16 19	66 79 75	6 5 6	33 22 23	63 74 69	4 4 7	26 18 23	69 75 72	5 7 4



Export Controls

INDUSTRY COALITION ON TECHNOLOGY TRANSFER
(ICOTT)

position statement on

ENCRYPTION EXPORT CONTROLS

David Peyton
Vice President
Information Technology Association of America
(ITAA)

June 7, 1993

Third Annual Conference on Cryptography

sponsored by

Computer Professionals for Social Responsibility
(CPSR)

Executive Summary

There is an important and growing need for data security products containing encryption in the private sector, both in the U.S. and overseas. Controlled encryption is increasingly used in over-the-counter software products, and as an element of larger hardware and software solutions.

The United States controls all encryption products for export. File encryption is controlled as a military item by the Department of State. As a matter of policy, a virtual embargo is in place for all exports of software containing file encryption to commercial customers other than banks, even to end-users located in countries that are America's closest allies.

Despite the fact that many types of software products containing encryption, particularly those in the public domain and those that are sold on a mass-market basis, are beyond effective control, and also the fact that many overseas vendors are now offering encryption, the U.S. has made no significant change in its approach to controlling these products. As a result, U.S. companies experience a loss in potential sales and increased legal risk with no commensurate benefit in terms of national security.

These problems can be addressed by maintaining the current general structure of controls, while 1) shifting public domain and mass-market software containing encryption (and related hardware products) to general license eligibility for non-terrorist and non-embargoed countries, and 2) allowing license approval for commercial customers in Free World countries.

1. WHAT IS ENCRYPTION?

Encryption (or cryptography) is a general term for techniques for keeping data secret. The primary method for accomplishing this is to apply mathematical or logical formulas to make data unreadable to those with unauthorized access. Such data may then be re-converted to readable form through the use of similar logic by those for whom the data is intended.

Encryption is used to protect data while it is in the process of transmission (e.g., over public or private networks), while it is stored and potentially unprotected (as in memory in portable computers or computer storage media), or while a computer system is actually in use, if some users of a system do not have authorized access to all data on the system. While not the only way to protect data, it is the backbone of data security systems for which a very high level of security is required. Other uses of encryption include "authentication," where encryption logic provides confirmation that a data user is who he claims to be. In such applications, the text of the message itself may or may not be encrypted.

2. WHY ENCRYPTION IS IMPORTANT

While the need for secure communications by government entities is well recognized, this need is just as important to a ever-widening range of organizations in the private sector. In general, any industry or activity that employs data communications and is dependent on valuable proprietary knowledge is vulnerable to unauthorized attempts to access that data.

Commercial activities that fall into this category are legion. The banking industry, for example, is a major market for encryption. In addition, non-banking industries with a history of industrial espionage such as petrochemicals and pharmaceuticals are also established markets. Due to the ubiquitous use of computer aided design and manufacturing (CAD/CAM), and the digitization and transmission of engineering data, a much wider range of industry, from automobiles to semiconductors, now use encryption for some aspect of data communications. Guides, manuals and other instructional materials dealing with encryption, as well as software packages themselves containing encryption functions, are common fare in retail software outlets in the U.S., Europe and elsewhere around the world.

Datapro Research estimated in 1991 that the U.S. market for data encryption "devices" alone exceeded \$150 million, with the overall market for data security (including hardware and software) estimated by Frost and Sullivan as exceeding \$1 billion. There are no reliable data for overseas demand, although market surveys by DATAPRO have revealed that overseas demand for encryption product, particularly in Europe, is increasing at a higher rate than in the U.S.

The U.S. intelligence community must be able to read data transmitted by actual or potential adversaries in order to avert threats to the national security. The National Security Agency exercises the primary mission within the U.S. defense and intelligence communities in addressing this need. However, NSA (through the vehicle of Department of State ITAR licenses) exerts stringent controls on all exports of file encryption outside of the United States and Canada, and imposes a virtual embargo of such items to commercial users other than banks, including those located in some of America's closest allies (e.g., Britain).

3. U.S. EXPORT CONTROLS AND ENCRYPTION

All software containing encryption is controlled for export from the U.S., either under the authority of the Export Administration Act or the Arms Export Control Act. A limited number of applications, primarily data authentication, specially designed banking applications, and decryption for copy-protected software, are controlled by the EAA, and are under the jurisdiction of the Department of Commerce. Such applications are readily exportable to destinations in the Free World, either under general or validated licenses.

Most file encryption is subject to control under the Arms Export Control Act, administered by the Department of State. Software containing file encryption, including software that is in the public domain or that is "mass-market" (by the internationally accepted COCOM definition) is subject to the same severe licensing regime as are tanks and missiles.

While the export licensing regime administered by the Department of State is slower, more restrictive and more cumbersome than that administered by the Department of Commerce, the key problem is licensing policy, not administration. The National Security Agency, which reviews export licenses and sets policy for export of encryption, routinely recommends denial of exports of encryption to commercial customers, even those located in America's closest allies. With the exception of a small number of weak encryption products, NSA will approve exports of file encryption only to nine allied governments, banks, and subsidiaries of U.S. companies. Thus, not only are these products subject to harsher controls, but there is a de facto embargo of them to America's major commercial data processing markets in Western Europe and Japan.

In part as a result of NSA's embargo policy, a data security industry has developed overseas free from competition from U.S. companies (particularly in their home markets) and completely free from U.S. export controls. Large multinationals as well as smaller specialized firms provide security products in response to growing demand, and make them available domestically without hindrance.

In response to recent attempts to decontrol mass-market software containing encryption, NSA has instituted a policy of releasing certain "mass-market" software to Department of Commerce control on a case-by-case basis. These products are limited to those based on particular proprietary algorithms (RSA's RC2 and RC4) of a limited key length. However, most encryption applications continue to be based on the National Institute of Standards and Technology's Data Encryption Standard (DES), which has been a Federal procurement standard since the late 1970's and has achieved wide acceptance among data security customers. As a result, the NSA procedure has had little impact in easing actual export restrictions.

3. NON-U.S. EXPORT CONTROLS

Export controls do exist on encryption among all of America's major allies; however, the nature and severity of controls varies significantly.

Britain

British companies are world leaders in encryption product; the market leader for encryption devices in the U.S. (Racal) is in fact a British company.

As encryption is not on the International (COCOM) Munitions List, Britain controls it as a dual-use, not a military, item. Consequently, both public domain software containing encryption and mass-market encryption software do not need a validated license for export, per the General Software Note of the COCOM agreement. While other encryption software remains subject to controls, the U.K. Department of Trade and Industry (with approval by General Communications Headquarters) will entertain license applications on a case by case basis.

Japan

Like Britain, Japan does not control either public domain or mass-market software containing encryption. The Ministry of International Trade and Industry will consider license requests for other encryption software on a case-by-case basis.

France

While France has decontrolled software that is in the public domain, like the U.S., it retains controls on "mass-market" and other encryption software as military items. Moreover, France requires licenses for the import of encryption into France.

Germany

Germany has specifically exempted encryption software from the General Software Note of the COCOM Industrial List, and retains controls on both public domain and "mass-market" software containing encryption.

Holland

Like the U.S., Holland controls all software containing file encryption as a military item.

Note that with the exception of France, none of these countries imposes restrictions on the use of encryption within its own borders (a list of major countries that do restrict imports is included as Appendix B). As a result, data security markets within these countries are reserved for local producers by the NSA-imposed embargo of U.S. products.

4. ISSUES IN EXPORT CONTROLS ON ENCRYPTION

Encryption Controls impact the computer industry in a number of important ways. For some companies, data security products are a major element of their product portfolios; for these, export controls directly affect the bottom line. However, such companies suffer only a small portion of the damage wreaked on U.S. industry as a result of current export licensing policy on encryption. The following cases demonstrate the major impacts that aspects of current controls have on the industry.

Case 1: Public Domain Software

The U.S. Munitions List controls software containing file encryption even if it is in the public domain. As a result, a number of products are available and widely distributed on international networks such as the INTERNET that contain ITAR-controlled encryption functionality. Software so available on the INTERNET can be accessed immediately nearly anywhere in the world and is thus beyond any effective control. While the Department of Commerce has long recognized this fact and decontrolled such software, NSA has retained nominal controls on such software containing encryption.

File encryption may not be a primary function of the software and may not be readily identified by summary software descriptions (example: DES-based encryption in the Berkeley Unix operating System). As a result, it may be downloaded for access by international users unknowingly, resulting in compliance exposure. Companies must incur overhead to screen thousands of public domain software applications for encryption in order to keep it out of their international networks and so avoid export compliance incidents.

Case 2: Mass-market Software

Software that is not in the public domain, but that is generally available to the public through retail channels and needs no significant support by the vendor ("mass-market" software) is beyond effective control. These packages are low-cost, marketed in the thousands or tens of thousands, and move readily across national borders over international computer networks and in personal baggage.

COCOM recognized both the practical limitations of controlling such software and the seriously adverse effects of maintaining controls. As a result, COCOM (with the U.S.) adopted the "General Software Note," which frees such software from validated licensing requirements. However, for U.S. export control purposes, this note does not apply to mass-market software containing encryption, even though the rationale for decontrol is just as valid. Moreover, stringent ITAR controls even in situations where sales may be permitted, are incompatible with the sale and physical accessibility of low-cost retail product.

As a result of this control, over-the-counter software vendors in the U.S. are forced to produce export versions of their products, even though the U.S. versions can be readily obtained through transmission from the U.S. over international networks and in personal baggage.. Large companies that support personal computers in particular must maintain expensive screening procedures to guarantee that the "U.S.-only" versions of common software products do not find their way into international price lists.

Another serious concern with controls on mass-market encryption has to do with the increasing use of notebook, lap-top and other portable P.C.'s. The need for an ITAR license for programs designed to encrypt stored data on such systems means that such data now goes unprotected on systems used by international business travelers. As a result, these systems are becoming the target of industrial espionage, a growing concern by corporate security managers.

Case 3: Source-Code Embargo on DOC-Controlled Encryption

The National Security Agency continues to require ITAR licenses for any encryption software that is exported in the form of source code, including code for functionalities that have been transferred to Department of Commerce jurisdiction. An example of such a function is "authentication," which is the use of encryption to provide assurance that an end-user is who he claims to be. Commercial uses of this functionality are extremely common.

When U.S. firms engage in joint ventures or co-development projects, software (such as operating systems) will often contain an authentication or other Commerce-controlled functionality. In order to engage in product development, source code must be transferred to the international partner. Under current NSA policy, source code for Commerce-controlled encryption requires an ITAR license, which will be denied if the partner is a commercial company. As a result, the code must be removed by the U.S. partner and re-written by the overseas participant. As the expertise to accomplish this is readily available in major Free World Countries, this recoding effort represents a significant, and unnecessary expense.

Case 4: Leveraged Sales

For many large computer companies, revenue from direct sale of data security products is limited; the market is in fact dominated by specialty firms. However, large sales are often dependent on the ability of U.S. firms to offer encryption as a feature of a customer solution involving hardware, software and services. Thus, if a U.S. firm is unable to offer an encryption solution, significant loss of revenue may result, even though the encryption/hardware and software element of the deal may be minor.

U.S. companies regularly encounter situations where the ability to offer encryption is key to a large project. Typical examples include replacement of corporate data systems, infrastructure projects such as PTT (post, telephone and telegraph) installations, and cellular telephone operations. For such projects, where customers perceive data security as necessary, they will be forced to look to a non-U.S. vendor for the entire project.

Due to the proliferation of data security vendors abroad, customers in such situations are increasingly looking to non-U.S. vendors for the encryption element of their MIS solutions; however, this only further dramatizes the disutility of current NSA policy.

5. Recommendations for Action

The computer industry recognizes the need to retain controls on encryption products in the interests of national security. However, a number of changes in current policy can be made to rationalize the current system while retaining controls on that which is controllable. The recommendations specified below in the form of legislative language will serve this end.

ENCIPHERMENT EXPORT CONTROL: PROPOSED LEGISLATIVE LANGUAGE

- A. Notwithstanding any provision of the Arms Export control Act or the Export Administration Act, no validated license may be required for the export or reexport of any software containing encryption capabilities that is
 - 1. Generally available to the public by being:
 - a. Sold from stock at retail selling points, without restriction, by means of:
 - 1. Over-the counter transactions;
 - 2. Mail order transactions;
 - 3. Telephone call transactions; and
 - b. Designed for installation by the user without further substantial support by the supplier; or
 - 2. In the public domain, or publicly available through being generally accessible to the interested public in any form.
- B. Notwithstanding any other provision of law, no validated license may be required for the export or reexport of any commodity solely because it incorporates or employs in any form software released from control by Part A.
- C. A validated license may not be required under the authority of the Arms Export Control Act for the export or reexport of software with encryption capabilities solely because such software is exported or reexported in the form of source code.
- D. The Secretary of State shall authorize the export or reexport of software containing encryption capability controlled by the Arms Export Control Act for non-military end-uses in any country to which exports of such software have been approved for use by financial institutions not controlled in fact by U.S. persons. The Secretary of State may not grant such authorization if there is substantial evidence that such encryption software will be diverted to a military end-use, or will be reexported without requisite U.S. authorization.

OBJECTIVES/RATIONALE

Part A

The intent of this Part is to provide GTDU treatment for software that is in the public domain, or that qualifies for "mass-market" treatment under the COCOM agreement. The language would provide licensing status for software containing file encryption identical to that which is now in force in Britain and Japan. However, the concept of "public domain" found in the COCOM agreement has been expanded to include software which is also "publicly available"- the basis for General License GTDA in the Export Administration Regulations.

Note that neither IEEPA nor the Trading With the Enemy Act are cited. This is to enable the continuation of controls on countries of terrorist concern (like Libya, Syria and Iran) or other embargoed countries (like Cuba and N. Korea). However, this language does intend to prevent the imposition of Section 6 EAA "foreign policy" controls.

Part B

Part B is intended to extend general license treatment to hardware implementations of software containing encryption that has been released because it is mass-market or in the public domain. However, such software may remain controlled for other reasons (e.g., the item in which the software is embedded or included is itself controlled).

Part C

Part D is intended to release source code of software that has been afforded general license treatment or that has been transferred to Commerce jurisdiction. However, such software could be controlled for other reasons. This language would apply to encryption software only.

Part D

Part D is intended to expand the current State Department/NSA policy of approving individual licenses and distribution agreement authority for the use of file encryption to financial institutions to other non-military customers in the same countries.

APPENDIX A

OVERVIEW OF PRODUCTS CONTAINING ENCRYPTION

The following list identifies some products (software and devices) produced outside of the United States providing encryption capability as a primary feature. It is intended to be illustrative of producers and products only. A dash (-) in the "algorithm" column indicates that the algorithm was not identified in product literature.

PRODUCT	MANUFACTURER	COUNTRY	ALGORITHM
Eracom Micro-Channel Slave Encryptor	Eracom Pty Ltd.	Australia	-
CRY12C102 DES CHIP	Cryptech	Belgium	DES
RAC/M II RAC/M	OkioK Data	Canada	DES
DES- C Imp; PC/PS 2 Imp;	Cryptomathic A/S	Denmark	DES
RSA- C Imp; PC/PS2 Imp			RSA
C544, C5420 C5430 SCSII Controllers Elkey 4 AT Elkey 4-LT Elkey 4- MCA	Computer Elektronik Infosys Gmbh	Germany	- DES
SAFE-Guard OS/2 Sign-Guard	Uti-Maco Software Gmbh	Germany	DES, RSA DES
Crypto3270 CryptoCom CryptoSafe	Algorithmic Research Ltd	Israel	DES, RSA DES, RSA DES
Concord-Eracom MFPS Card PC Encryptor	Concord-Eracom Nederland	Netherlands	DES DES
P9825 (CS/X) Crypto Server	Philips	Netherlands	DES
Cryptos	Askri	Russia	DES, RSA
NETCrypt PCrypt	Sonnor Crypto AB	Sweden	HR&S(prop.) HR&S

SC3600	British Telecom	U.K.	DES, B-Crypt
Lektor 3610			DES, B-Crypt
Lektor 3620			DES, B-Crypt
Lektor 3630			DES, B-Crypt
Ultralock	Business Simulations	U.K.	-
X-soft 10	Compuserve	U.K.	-
S3500	Computer Security Ltd.	U.K.	DES, prop.
S7500			DES, prop.
S7700(X.25)		U.K.	DES, prop.
S8100			DES
PC-Guard			-
rsaSIGN/rsaCHECK			-
CG500	Data Innovation Ltd.	U.K.	-
ED500			DES
ED600		U.K.	prop.
ED2048		U.K.	DES, prop.
PCP400		U.K.	DES, prop.
Cryptopad	Dynatech Communications	U.K.	DES,
Cipher 2200			CODEP(prop.)
Multicrypt			CODEP
			DES,
			CODEP(prop.)
Datasave-ABA;	International Data	U.K.	-
Key Management	Security		-
Gatekeeper			-
Protec			-
Virus-PRO			-
Watchdog	IT Security International	U.K.	-
Kinetic Access II	John Vale	U.K.	-
Datalock	JPY Associates	U.K.	DES
PC-Audit	Microexpert	U.K.	-
CLAM	Microft	U.K.	Prop.
MenuGen+D-Lock			-
Trispan	Micronyx	U.K.	-
Triumph!			-
Stoplock I-S	PC Security	U.K.	-
Stoplock II			-
Stoplock III			-

Datalok-H	Plessey Crypto	U.K.	-
Datalok-L			-
FAXLOK			-
FTSM 100			RSA
NC100			
Voicelok 100			-
SAFE-Guard	Prosoft Limited	U.K.	DES, RSA
RG600, PC	Racal-Guardata	U.K.	-
Security Module; RG700 PC			
Security Module	Note: These products		
RG6000 Host	are offered for		DES
Security Module	sale in the U.K.		
RG9000 X9			
Cryptoserver			
RG1000 RSA Utility for IBM Mainframe			RSA
Activator/S	Software Security	U.K.	-
CRYPTO-JET	Sophos Ltd.	U.K.	DES
DES TOOLKIT			DES
EDS			DES, SPA
PUBLIC			DES, RSA, MDH
PURGE			DES
RSA TOOLKIT			RSA
SHRED			DES
VACCINE			-
DES-LOCK	Sypro	U.K.	-
Datalock One (DLK-1)	Zergo	U.K.	-
DL4000			-
PSP400			-

APPENDIX B

IMPORT CONTROLS ON ENCRYPTION

The following countries exercise import restrictions (require an import permit or license) on encryption hardware and software:

Australia (at the request of exporting
country)

France
Hong Kong
Israel
Singapore

The following countries have no restrictions on the import of encryption:

Belgium
Brazil
Germany
Italy
Malaysia
Netherlands
Spain
Sweden
Switzerland
Taiwan
Thailand
United Kingdom



1730 M Street
Northwest
Suite 700
Washington, DC
20036-4510

Telephone
(202) 452-1600

Fax
(202) 223-8756

TESTIMONY OF

ILENE ROSENTHAL

GENERAL COUNSEL

SOFTWARE PUBLISHERS ASSOCIATION

ON

NATIONAL CRYPTOGRAPHIC POLICIES

BEFORE THE

COMPUTER SYSTEMS SECURITY AND PRIVACY ADVISORY BOARD

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

June 3, 1993

Gaithersburg, Maryland

Introduction And Summary

I am Ilene Rosenthal, General Counsel of the Software Publishers Association ("SPA"). SPA is the principal trade association of the personal computer software industry. SPA's over 1,000 members represent the leading publishers in the business, consumer and education software markets.

America's software companies are bright spots in this otherwise dull economy and are among the country's most internationally competitive firms. American PC software publishers currently hold a 75% worldwide market share. Export sales average more than 40% of revenues and are greater than 50% for larger companies.

We greatly appreciate the opportunity to testify before you today. We believe that the Administration's April 16th announcement of an interagency study of encryption technologies and policies provides an excellent and expedited opportunity to move forward with significant liberalization of export controls on mass market software with encryption capabilities. Existing "munitions" export controls which prevent our members from offering DES and other comparable strength encryption algorithms continue to significantly harm our members. Indeed, we have become even more concerned as SPA's recent research has revealed the full extent to which foreign customers can turn to foreign suppliers to meet their encryption needs. Moreover, the Administration's recent "Clipper

Chip" proposal does not address our concerns and should not be allowed to be an excuse to delay further export liberalization of mass market software using DES or other algorithms such as RC2/RC4 at comparable strengths.

SPA's Recent Research Reveals A Robust and Rapidly Expanding Foreign Market In Encryption Software and Hardware.

Some government officials routinely assert that even if the Government were to prohibit America's software publishers from offering encryption features demanded by their customers abroad, we should not be concerned because there are no foreign programs and products available. Such an assertion is erroneous. Indeed, as I will explain, there are a very large number of such programs and products available on the market today.

Because of the confusion and misinformation in this area, during the last three weeks an SPA research team surveyed commercially available foreign encryption software, hardware, and combination products. Team members were selected based on their knowledge about computer hardware and software capabilities and requirements, information security, and cryptology.

I want to emphasize that we only included programs and products that provided data, text and file encryption capabilities.

We excluded voice encryption products, and programs or products that simply provided access control or authentication. Moreover, our focus has been on programs and products using strong encryption -- DES or its equivalent.

Our initial information came from our members, industry surveys, trade publications, press reports, sales literature and other materials. Team members then reached out to companies around the world through phone and fax to clarify exactly what their products were, what they did, what the hardware requirements were, how we could purchase the program or product, whether the export version was the same that was sold domestically, etc. This allows us is to categorize with some certainty what we are talking about.

As you might expect, this process is time-consuming and probably will take several weeks to complete. Nevertheless, today I did want to report our preliminary results.

- The U.S. no longer dominates the encryption field. In fact, SPA has identified to date more foreign than domestic encryption programs and products (143 versus 133). Not surprisingly, our initial compilation of the foreign programs and products was skewed towards those in English speaking countries; thus we believe additional research will reveal even larger numbers.

- We have confirmed the availability of 80 foreign software, hardware and combination products for text, file, or data encryption, from companies in 13 foreign countries (Israel, United Kingdom, Netherlands, Denmark, Switzerland, Ireland, Canada, Sweden, Germany, Belgium, France, Australia and South Africa).¹ 48 employ DES. 63 additional foreign encryption programs and products have been identified (including those from an additional five countries) but have yet to be investigated. However, we believe many of these also will be found to employ DES or other comparable strength encryption algorithms.
- We have confirmed the availability of 15 foreign mass market encryption software programs and kits which employ the DES algorithm. These are published by companies in Germany, Israel, United Kingdom, Denmark, Canada, Belgium and Australia. We know some have distributors in other foreign countries and in the United States; one, a U.K. company, has distributors in 9 countries (Bahrain, Singapore, Ireland, Greece, Italy, Malta, Netherlands, Spain, Norway). The

¹ Hardware and combination products are appropriate to include in any determination of the foreign availability of encryption programs and products. In the PC market, the foreign hardware encryption is typically implemented in the form of an expansion board/card. These products satisfy the mass market definition and their ease and acceptability is demonstrated by the large number of commercially available boards for enhanced video, expanded memory, fax modem capabilities, printer ports, game ports, and sound cards (e.g. "Sound Blaster").

programs are installed by the user inserting a floppy diskette; the kits enable encryption capabilities to be easily programmed into a variety of applications.

- . Foreign companies increasingly recognize and are responding to the need to provide software only encryption solutions. Although the foreign encryption market is still heavily weighted towards encryption hardware and hardware/software combinations, the market trend is towards software for reasons of cost, convenience and space. For example, one German company which traditionally sold DES hardware told us it had just come out with its first DES software implementation. Another German company has developed a "smart diskette" -- encryption hardware that comes in the form of a floppy diskette.

I had hoped to be able to actually show you today copies of at least the foreign mass market DES encryption software programs, and perhaps an expansion board or two. We had several vendors ready, willing and eager to ship to us, and their government would let them do so. However, it may come as a surprise to you that the Arms Export Control Act not only prohibits Americans from exporting DES-based programs, but is also the basis for restricting

"munitions" imports. Because mass market software with encryption capabilities remains on the U.S. Munitions List -- even though it is not on the COCOM Munitions List -- we would need an import license from the Department of State/NSA. If our experience on the export side is any guide, it would take weeks if not months to obtain such a license.

In addition to these commercially available programs and products, any analysis of the availability of foreign encryption alternatives must consider programs available on the Internet, which is the largest global network connecting millions of users throughout the world.

- DES is widely available on the Internet including implementations that can be simply down-loaded and used. There are even available archives of DES implementations. We reviewed one such compilation in the U.S. which revealed 16 DES implementations. We also reviewed an archive in Finland which revealed 2 DES implementations; in Italy with 4 DES implementations; and in Australia with 3 DES implementations. John Gage, of Sun Microsystems, recently testified at a hearing of the House Telecommunications & Finance Subcommittee chaired by Rep. Markey regarding the ease with which a DES implementation can be downloaded.

- The recently popularized Pretty Good Privacy (PGP) software program also is widely available throughout the world. PGP implements the International Data Encryption Algorithm (IDEA). The program is intended for electronic mail, but also is ideal for encrypting files. It is available for free and may be used legally throughout Europe, whether in a business or at home. IDEA was developed by a well-known Swiss cryptographer, James L. Massey, and provides encryption protection comparable to DES. Indeed, we understand it may become the basis for a European standard. Moreover, we understand a respected cryptologist in this country, Peter Schweitzer, examined IDEA and preliminarily concluded that he would prefer it to using DES in the immediate future! (He has submitted his views to NIST.) PGP software is available both in source code form and as ready-to-run executable programs for DOS and MacIntosh Operating Systems. It comes with easy-to-read instructions, is trivial to install, and simple to use. We understand the entire process of logging in, downloading the program and logging off takes about three minutes. To get some idea of its availability, we stopped after identifying 50 different Internet sites around the world that carry PGP software including locations in Finland, Germany, Canada, Sweden, and the UK. (Apparently IDEA also has been implemented in an integrated circuit chip called "Vinci.")

In short, unilateral U.S. export controls hardly make any sense given the widespread legal availability of foreign encryption programs and products. Foreign companies will buy foreign products if they cannot buy from American companies and in turn become ex-U.S. customers. As a result, the U.S. Government will succeed only in crippling an American industry's exporting ability.

America's Software Publishers Are Directly Harmed By Existing Export Controls.

At an April 23 Administration briefing on the Clipper Chip, an FBI representative was asked how many of the approximately 800 authorized wiretaps executed by law enforcement officials in 1992 encountered encryption (i.e. is encryption prevalent?). The FBI representative responded that while very few wiretaps encountered encryption, the FBI anticipated that they would increasingly encounter encryption in the near future. This point was sharpened by Ray Kammer, NIST's Acting Director, who added that we are indeed on the brink of a technological revolution. This is our point exactly: demand for encryption is significant and will grow rapidly.

There can be no doubt that foreign customers want first-rate encryption. According to the marketing and sales people in SPA's member companies, the demand for tough encryption among large domestic, foreign and multi-national companies and institutions in

the financial, telecommunications, health care, utilities and other industries (and among government agencies) is "extremely high."

Existing survey results support this conclusion. For example, earlier this year, BIS Strategic Decisions of Norwell, Massachusetts, polled thirty companies that either were existing electronic mail users or planned to implement E-mail within the next 24 months. The survey was split between large and small companies and covered a variety of industries. BIS found that security was viewed as the most important of 17 features of an E-mail system for all companies.

Similarly, in late 1991 the Business Research Group of Newton, Massachusetts, interviewed the data center managers at 200 of the Fortune 500 companies. All said they believed security issues were important; 65% said security was extremely important and the remainder said somewhat important. More than half had undertaken data encryption among their security measures.

There are at least four reasons why the demand for encryption has grown and, even more importantly, why it can be expected to continue increasing in the future. First, more sensitive information is being kept on PC networks. Second, advances in computing power make possible, at lower cost, "brute force" (random) attacks in which every key is tried until the text is intelligible. Third, there is a much greater awareness among PC

users of the dangers presented by hackers and viruses. Finally, several technological developments have occurred which are now favoring encryption via software rather than hardware.

Because America's software publishers have not been able to offer their foreign customers the tough encryption they are demanding, America's companies have lost sales. Moreover, even if a sale proceeds, our members have explained that they then have a dissatisfied foreign customer because they realize they have a product employing "crypto lite." The government already has one surrogate for lost sales and dissatisfied customers: the number of State Department/NSA export license applications denied, modified, or withdrawn. However, attempting to quantify lost sales is a misguided mission because many potential customers know U.S. companies can't meet demand and so no longer inquire. Conversely, some of our members tell us they have given up even trying to get export approvals for DES, etc. to meet customer demand.

For example, because of existing export restrictions, an American company recently found itself unable to export a mass market software program which provided encryption using Canadian technology based on a Japanese algorithm. Yet other European and Japanese companies are selling competing products world-wide using the same Canadian technology! Another SPA member's product manager in Europe reported the likely loss of at least 50% of its business among European financial institutions, defense industries,

telecommunications companies and government agencies if present restrictions on key size are not lifted. Yet another SPA member company reported the potential loss of a substantial portion of its international business if it cannot commit to provide DES in its programs.

The history of successful American software companies shows that they have identified a customer demand not currently being met by existing software publishers and have been early in the race to exploit this market niche. They then build on this toe-hold to broaden their operations. The same scenario faces us today: while foreign companies market software and hardware devoted to encryption, they will rush to develop broader application programs and products which incorporate encryption capabilities and therefore are more user friendly than a "layered" approach.

It would be a fundamental failure of American trade and export policy if industry was forced to show loss of market share before our Government did anything. Customers lost are never easily regained. Our Government should not force American companies to play "catch up." By failing to act now to liberalize export controls, our Government is directly harming the world-wide preeminent position of one of America's star exporting industries and threatening America's technological leadership in this area.

The Clipper/Capstone Chip Proposed Regime Must Not Be Used As An
Excuse To Delay Further Export Liberalization

As you know, on April 16, 1993 the Administration proposed a specific regime for the encryption of electronic communications in the United States.

In brief, the proposal involves using encryption microcircuits (so-called "Clipper Chips") embodying an NSA-developed classified algorithm which will be manufactured by government contractors in secure facilities. In addition, the "key" necessary to decrypt communications using these chips will be split into two parts and each part will be held in escrow by government agencies or other third parties, accessible to law enforcement and intelligence agencies pursuant to a court issued warrant.

Obviously there are a great number of companies, organizations and associations which will be testifying on various aspects of the government's proposals. I would like to focus on the possible implications for the prospects of further export liberalization.

As you know, for over two years SPA has urged that U.S. export controls on mass market software with encryption capabilities be liberalized. We fear that the Administration will attempt to "satisfy" this demand by at some point announcing that it will approve exports of hardware employing the Clipper Chip. At the

same time, the Administration would refuse to liberalize export controls on other encryption hardware and software arguing that it had provided a reasonable alternative to American companies. The implications of this position are deeply troubling.

First, we think any discussion of the Administration's proposal has to be premised on the fact that the Administration intends to preclude the use domestically of alternate forms of encryption. Otherwise the proposal simply has limited effect. Legitimate users would undoubtedly choose hardware or software which performed better, was cheaper and did not involve escrowed keys. Even if someone did use a clipper chip, there would be nothing to preclude the encryption of voice or data before its encryption via the clipper chip. Moreover, clearly if there are alternatives, the smart criminal will choose them rather than something that law enforcement holds the key to. Quite simply, the proposal is nonsensical if postulated as "voluntary." Moreover, even if made mandatory, there always will be encryption alternatives available to those of criminal intent and technical inclination.

Second, however, any encryption regime that requires all data to be encrypted via hardware has significant disadvantages. As we have testified, our customers are demanding encryption through software for reasons of cost, convenience, scarce computer "real estate", and particular performance requirements. We also have

shown you the widespread availability of encryption software. Yet we have not heard of how a Clipper Chip could be implemented in software and have serious doubts that it could be.

Third, a system in which the U.S. Government holds or has access to the keys will not be accepted by foreign (or U.S.) customers. It strains credulity to think otherwise. Indeed, I note that NIST's Acting Director, Ray Kammer, testified before the House of Representatives last month that if he were a foreign customer he wouldn't buy encryption using the Clipper Chip. Thus, if the Clipper Chip proposal is made mandatory, then whether or not NSA permits its export, the Government will have de facto adopted a policy whereby American companies are restricted to selling to the domestic market.

This is extremely troublesome. But it is not surprising. NSA has suggested to us on prior occasions that perhaps the "correct" solution is to divide the world into national markets. Yet we seriously question whether the way to remedy America's persistent trade deficit is to restrict exports by one of our most internationally competitive industries!

Conclusion

We appreciate the opportunity to testify before you today. We hope that your work and input into the interagency review process

will lead to immediate and significant export liberalization on mass market software with encryption capabilities. Such liberalization is warranted given the exploding foreign demand for encryption, the wide-spread availability of encryption products, and the significant and direct harm posed for one of America's most important and competitive industries.

Thank you.

**PRELIMINARY LIST OF FOREIGN
FILE, DATA & TEXT ENCRYPTION
PROGRAMS & PRODUCTS
CONFIRMED BY SPA (as of 6/2/93)**

Foreign Mass Market Encryption Software

<u>Software Manufacturer</u>	<u>Country</u>	<u>Product Name</u>	<u>DES</u>
Algorithmic Research Ltd	Israel	AR DISKrete	no
Algorithmic Research Ltd	Israel	Crypto3270	yes
Algorithmic Research Ltd	Israel	CryptoBIOS	yes
Algorithmic Research Ltd	Israel	CryptoCom	yes
Algorithmic Research Ltd	Israel	CryptoMAIN	yes
Algorithmic Research Ltd	Israel	CryptoPC	yes
Bysoft	Canada	Cryptoflex	yes
CE Infosys	Germany/USA	SoftCrypt	yes
Cryptech	Bel/Neth/Fra	DES Software Toolkit	yes
Cryptomat (h) ic	Denmark	DES	yes
Cryptomat (h) ic	Denmark	F2F	yes
DataSoft Ltd	UK	Datataalk/Datacode	no
Incaa Datacom	Netherlands	AUTHORIZER	yes
Microft Techno Ltd	UK	CLAM	no
Sophos Ltd	UK	DES Toolkit	yes
Sophos Ltd	UK	EDS	yes
Sophos Ltd	UK	PUBLIC	yes
Effracom Pty Ltd	Australia		yes

Foreign Hardware and Hardware/Software Hybrid

<u>Software Manufacturer</u>	<u>Country</u>	<u>Product Names</u>	<u>DES</u>
Algorithmic Research Ltd.	Israel	AR CryptoSafe	yes
Ardy Elektronik AB	Sweden	SLD-OUS 200	no
CE Infosys	Germany/USA	C5420/30/40	yes
CE Infosys	Germany/USA	CryptCard	yes
CE Infosys	Germany/USA	MiniCrypt	yes
CE Infosys	Germany/USA	SC8810/20	yes
CE Infosys	Germany/USA	SuperCrypt	yes
Concord Eracom	Netherlands	MFPS Encryptor	yes
Concord Eracom	Netherlands	SecNet FBI-Encryptor	no
Cryptech	Bel/Neth/Fra	DES-CHIP	yes
Data Innovation Ltd	UK	ED500	yes
Data Innovation Ltd	UK	ED600	no
Data Innovation	UK	ED2048	yes
Dynatech Communications Ltd	UK	Cipher 2200	no
Dynatech Communications Ltd	UK	Cryptopad	yes
Dynatech Communications Ltd	UK	Cybercrypt LE	yes
Dynatech Communications Ltd	UK	Multicrypt	yes
Ecole Polytechnique	Switzerland	VINCI	no
Eracom Pty Ltd	Australia	MCSE-16	yes
Eracom Pty Ltd	Australia	MCSE-8	yes
Eracom Pty Ltd	Australia	PCE-16	yes
Eracom Pty Ltd	Australia	PCE-8	yes

Foreign Hardware and Hardware/Software Hybrid (cont'd)

<u>Software Manufacturer</u>	<u>Country</u>	<u>Product Names</u>	<u>DES</u>
Eracom Pty Ltd	Australia	ERA 2007	yes
Eracom Pty Ltd	Australia	ERA 4007	yes
Eurologic Systems	Ireland	Datacrypt	no
GEC-Marconi Secure Systems	UK	Datalok H	no
GEC-Marconi Secure Systems	UK	Datalok L	no
GEC-Marconi Secure Systems	UK	Marcrypt	no
Gretag AG	Switzerland	Gretacoder 522	yes
Gretag AG	Switzerland	Gretacoder 524	yes
Gretag AG	Switzerland	Gretacoder 528	yes
Gretag Ltd	UK	Greatcoder 606	yes
Info Guard AG	Switzerland	I-1100	yes
Info Guard AG	Switzerland	I-2010	no
Info Guard AG	Switzerland	I-3010	no
Intelligent	S.Africa		
Jaguar Communications	UK	Z-CODA-A	no
Jaguar Communications	UK	Z-CODA-X	no
Mobius Enc Techno	Canada	FaxSecrets	no
Mobius Enc Techno	Canada	TradeSecrets	yes
Nanoteq	S. Africa		
Net One	S. Africa		
News Datacom	Israel	N-Sure Access 1000	yes
Northern Telecom	Canada/US/UK	PDSO	yes
Okiok Data	Canada	RAC/M II	yes
Omnisec AG	Switzerland	Omnisec 810	no

Foreign Hardware and Hardware/Software Hybrid (cont'd)

<u>Software Manufacturer</u>	<u>Country</u>	<u>Product Names</u>	<u>DES</u>
Omnisec AG	Switzerland	Omnisec 820	no
Omnisec AG	Switzerland	Omnisec 830	no
Omnisec AG	Switzerland	Omnisec 840	no
Plessey	UK	DataLock	yes
Plessey	UK	FaxLock	yes
Plessey	UK	VoiceLok	yes
Racal Milgo	UK	modems	no
SecuriCrypto AB	Sweden	SecuriCryptoX.	no
Spescom	S.Africa		
TRAC Systems	Australia		yes
Tecnetics	S. Africa	N3000SM	yes
Tele Security Timmann	Germany	TST 5573 C	no
Tele Security Timmann	Germany	TST 5573 H/C	no
Tele Security Timmann	Germany	TST 5573 PC	no
Tele Security Timmann	Germany	TST 5573 X/C	no
Zeta Communications Ltd	UK	Zetacode A	no

Dr. Vinton G. Cerf
3614 Camelot Drive
Annandale, VA 22003-1302

11 April 1993
The Honorable Timothy Valentine
Committee on Science, Space and Technology
Subcommittee on Technology, Environment and Aviation
House of Representatives
Rayburn House Office Building

Dear Chairman Valentine:

I recently had the honor of testifying before the Subcommittee on Technology, Environment and Aviation during which time Representative Rohrabacher (R, California) made the request that I prepare correspondence to the committee concerning the present US policy on the export of hardware and software implementing the Data Encryption Standard (DES) and the RSA Public Key encryption algorithm (RSA).

As you know, the DES was developed by the National Institute for Standards and Technology (NIST) in the mid-1970s, based on technology developed by International Business Machines (IBM). The details of the algorithm were made widely available to the public and considerable opportunity for public comment on the technology was offered. In the same general time period, two researchers at Stanford University (Martin Hellman and Whitfield Diffie) published a paper describing the possible existence of mathematical functions which, unlike the symmetric DES algorithm, could act in a special, pairwise fashion to support encryption and decryption. These so-called "public key algorithms" had the unusual property that one function would encrypt and the other decrypt -- differing from the symmetric DES in which a single function performs both operations. The public key system uses a pair of keys, one held private and the other made public. DES uses one key which is kept secret by all parties using it.

Three researchers at MIT (Rivest, Shamir and Adelman) discovered an algorithm which met Hellman and Diffie's criteria. This algorithm is now called "RSA" in reference to its inventors. The RSA technology was patented by Stanford and MIT and a company, Public Key Partners (PKP), created to manage licensing of the RSA technology. A company called RSA Data Security, Inc., was also formed, which licensed the technology from PKP and markets

products to the public based on the technology.

The current policy of the United States places DES and RSA technology under export control. Because cryptography falls into the category of munitions, it is controlled not only by the Commerce Department but also by the State Department under the terms of the International Traffic in Arms regulations. Despite the public development of both of these technologies and their documented availability outside the United States over the last 15 years, US policy has been uniformly restrictive concerning export licensing.

As the United States and the rest of the world enter more fully into the Information Age in which digital communications plays a critical role in the global infrastructure, the "digital signature" capability of public key cryptography is a critical necessity for validating business transactions and for identifying ownership of intellectual property expressed in digital electronic forms.

Registration and transfer of intellectual property rights in works which can be represented in digital form will be central factors in the national and global information infrastructure. A number of parties are exploring technical means for carrying out rights registration and transfer, making use of public key cryptography as a basic tool.

In addition, there is a great deal of current work on electronic mail systems which support privacy by means of encryption and support authenticity by means of digital signatures. One of these systems, developed in the Internet environment I mentioned in my testimony, is called Privacy-enhanced Mail (PEM) and makes use of DES, RSA and some other special "hash" functions which are integral to the production of digital signatures.

For these various systems to be compatible on an international basis, it would be very helpful for the cryptographic components to be exportable on a world-wide basis. A number of vendors make products relying on these technologies within the United States but often find it very difficult to engage in international commerce owing to the export licensing required for these technologies. Ironically, the technology appears to be widely available outside the US and also outside the COCOM countries, so US firms face both competition outside the US and export inhibitions in their attempts to develop worldwide markets.

There are many valid national security reasons for limiting the export of cryptographic capabilities, since these technologies may aid an opponent in time of war or other conflict. Perhaps just as important, US intelligence gathering capability can be eroded by the availability of high grade cryptography on a worldwide basis. Recently, it has also been alleged that the world-wide availability of cryptography would also seriously impede US drug enforcement and anti-crime efforts. While these reasons seem sufficient, many have pointed out that the widespread accessibility to the detailed specifications of DES and RSA and availability and existence of software and hardware outside the US have long since done whatever damage is going to be done in respect of warfighting, crime or drug potential. This line of reasoning leads to the conclusion that our policies only inhibit legitimate commerce, but have little impact on the other concerns expressed.

As in all such controversy, there is often some truth on both sides. The National Institutes of Standards and Technology (NIST), has offered alternative digital signature capability. Technical assessments of the alternative have turned up weaknesses, in the opinions of some experts. There is not yet an alternative to DES, unless it is to be found in NSA's Commercial Crypto Evaluation Program (CCEP) in which NSA proposes to provide algorithms which are implemented in hardware by industry and made available for civilian use. As I understand this program, NSA does not intend to release any details of the algorithms, leaving open questions about the nature and strength of the technology. Some experts will persist in the belief that such offerings have weaknesses which are deliberately built in and hidden (so-called "Trojan Horses") which will allow the agency to "break" any messages protected by this means.

The critics complained loudly that the reasoning behind the design of certain parts of the DES algorithm (specifically the "S-boxes") was never made public and therefore that the algorithm was suspect. In fact, the DES has proven to be very strong - indeed, it may be that very fact which makes it so unpalatable in some quarters to permit its unrestricted export. It may be that the CCEP technology offered is satisfactory, but this is hard to tell without knowing more about its provenance.

Presuming the wide availability of both DES and RSA technology, it seems to me appropriate and timely to re-examine US export control policy regarding these two algorithms. In all probability, any such review will require some classified testimony which will have to be heard in confidence by cleared members of your committee. I sincerely hope that the outcome will be favorable to use by US industry in international commerce, but even if the outcome results in continuation of present policy, it is timely to make such a review, in my opinion.

Sincerely,

Vinton G. Cerf



SOFTWARE
PUBLISHERS
ASSOCIATION

1730 M ST.
NORTHWEST
SUITE 700
WASHINGTON, DC 20036
TEL: 202-452-1600
FAX: 202-223-8756

FOR IMMEDIATE RELEASE

Contact: Ilene Rosenthal, General Counsel
Terri Childs, Public Relations Manager
(202) 452-1600

SPA Supports Relaxed and Streamlined Export Controls of Encryption Software Issued by Bush Administration

July 17, 1992 (*Washington, DC*)—After extensive discussions between the Software Publishers Association (SPA) and the Bush administration, the Administration will relax and streamline export controls of mass-market software with encryption capabilities. These changes will provide enhanced information security for business needs and ensure individuals greater levels of privacy in communications than have been available to date.

"The US Government has taken a significant first step in addressing the global commercial needs of US software publishers by allowing publishers to include significantly stronger encryption capabilities in the mass-market programs they export than presently permitted," stated Ken Wasch, SPA Executive Director. "The changes will help ensure the continued vitality of one of America's star exporting industries."

The new substantive criteria and expedited export review process were set forth in new regulations and in a letter to key members of Congress from the President's National Security Advisor, General Brent Scowcroft.

—more—

July 17,1992

Under the new system the Administration will grant export approval within 7 days of request for software using two of RSA Data Security Inc.'s algorithms, RC2 and RC4. Most of the major US software publishers already have licensed these algorithms. In addition, RSA's new license fee schedule puts these algorithms within the reach of all companies. Other proprietary algorithms also may continue to be used but now will be reviewed on a streamlined case-by-case basis. However, despite SPA efforts, the Administration refused to change the current restrictions on the export of programs using the Data Encryption Standard (DES).

The Administration also has agreed to hold semi-annual meetings with the industry, the first of which will be hosted by General Scowcroft in early September, 1992. These meetings will address the continued suitability of the technical criteria, including whether the algorithms and/or bit lengths need revision to reflect encryption developments and advances in computing power and speed. The meetings will also address whether or not foreign availability of mass-market software with encryption places US companies at a competitive disadvantage.

"This victory for the software industry is due in large part to the efforts of several members of Congress," stated Karen Casser, SPA Director of Public Policy & Legal Affairs. "In particular, Congressman Mel Levine (D-CA) as well as Representatives Sam Gejdenson (D-CT), John Miller (R-WA), Bill Orton (D-UT), and Wayne Owens (D-UT) were instrumental in passing the House bill. Also, Senator Jake Garn (R-UT) was able to gain the attention of General Scowcroft. These efforts acted as a catalyst to focus Administration attention on the issue."

The Software Publishers Association is the principal trade association of the personal computer software industry. Its over 900 members represent the leading publishers in the business, consumer, and education software markets. The SPA has offices in Washington, DC, and Paris, France.

#

(Please Note: Background briefing paper is attached. To obtain more detailed information about this issue, please contact the SPA PR Department at (202) 452-1600, x320 and request the "Encryption/Export Controls Package.")

July 17,1992

Encryption Background

American PC software companies are among the country's most internationally competitive firms. Export sales average more than one-third of revenues and are greater than 50% for some larger companies.

These companies are publishing an increasing number of mass-market software programs with encryption capabilities. The programs are developed to meet the rapidly growing commercial demand in the US and abroad for protection of corporate communications and files against unauthorized access, alteration, and appropriation. Indeed, within the next 5 years, a substantial majority of all mass-market programs will include data, text and file encryption capabilities, in addition to simpler password and access control features.

These mass-market software programs may be used with any personal computer and can be purchased at thousands of retail outlets (e.g., Egghead Software), by mail, over the phone, etc. Yet exports of such mass-market programs with encryption capabilities are controlled as "munitions" under the Arms Export Control Act. They must be cleared through a laborious case-by-case process with the State Department's Office of Defense Trade Controls, which submits the software to the National Security Agency ("NSA") for review. The restrictive controls continued despite a decision by COCOM over a year ago that **all** mass market software—including software with encryption capabilities— should be controlled as are other commercial, dual-use items. If this were the case, export controls would be imposed only if exports of all software were restricted—but would **not** be imposed merely because the software had encryption capabilities.

The SPA argued vigorously that strictly controlling exports of software with encryption capabilities does **not** protect national interest because such programs in fact become available abroad anyway as soon as they become available in the United States. Either individuals leave with a floppy disk or simply transfer the program to a foreign computer via a telephone modem.

—more—

July 17,1992

At the same time, the SPA has explained that continued restrictive export controls do significantly harm the legitimate export prospects of America's software publishers. Not only is there the direct time and expense of the export license procedure, but software developers are never sure their program will meet with approval, and sales are lost to foreign competitors during the delays.

The result is to hand foreign markets to foreign suppliers and increase the incidence of piracy of US software products. A tremendous amount is at stake. Unless American software publishers are able to meet user demands for programs providing information security, within 5 years an annual export market of \$3-\$5 billion will be lost to foreign suppliers—at a cost of 60,000 to 100,000 jobs.

"The long-standing reluctance of the Administration to address this issue resulted in the industry seeking a legislative solution," said Bruce Heiman, of Preston Gates Ellis & Rouvelas Meeds, SPA's outside counsel. SPA sought a legislative remedy, and Rep. Mel Levine (D-CA) included a provision in the House-passed Export Administration Act (EAA) Reauthorization bill (H.R. 3489). This provision would have effectively decontrolled such software by shifting responsibility for review and approval of export licenses for software with encryption capabilities from the State Department's Office of Defense Trade Controls to the Commerce Department.

The Administration, however, threatened to veto any EAA bill that includes the Levine provision. Thus, industry members were encouraged by Congress to discuss possible administrative changes to the existing arms export control process directly with the Administration. "The administrative changes announced today represent real progress and obviate the need for legislation at this time," said Heiman.

#

THE WHITE HOUSE

WASHINGTON

Dear Senator Garn:

I am pleased to advise you that we have, with representatives of the mass-market software publishers industry, developed changes to the Arms Export Control Act (AECA) regulations and procedures to address the software publishers' concerns regarding export control of mass-marketed software with encryption.

As you know, the legislation the House passed in the First Session of the 102nd Congress reauthorizing the Export Administration Act (EAA) (H.R. 3489) included a provision that would remove mass-market software with encryption from the export control jurisdiction of the AECA and place it under the jurisdiction of the EAA. This provision, added with the expectation that shifting commodity jurisdiction for this technology would result in its decontrol, was in response to the software publishers' concerns that existing controls and procedures damage the competitiveness of the U.S. software publishers. The Administration had serious concerns that such a shift in jurisdiction could jeopardize activities critical to the national security.

At your urging, and in the interest of enacting appropriate legislation reauthorizing the EAA, Administration representatives met with publishers of mass-market software with encryption to determine if there were steps that could be taken to accommodate their concerns, while maintaining this critical technology under the commodity jurisdiction of the AECA. This meeting led to discussions with representatives of the Software Publishers Association (SPA). They outlined their concerns with existing AECA controls and their interest to relax these controls and to have a procedure to permit a more predictable and expeditious transfer of the commodity jurisdiction of certain mass-market software with encryption capabilities from the Department of State to the Department of Commerce on the Commodity Control List.

In response to these discussions, we have agreed to establish a procedure, under the AECA, by which requests to transfer mass-market software products that implement agreed upon encryption algorithms with specified key lengths will be expeditiously reviewed and transferred from the Department of State to the Department of Commerce on the Commodity Control List. The Department of State shall respond to inquiries regarding these new procedures within one working day and shall process each request within seven working days. We will work with the industry to alert mass-market software publishers and vendors of

these new procedures. Companies may continue under the existing procedures to develop exportable software products that implement other encryption algorithms. These also will be handled subject to specified time limits. All encryption products previously transferred to EAA jurisdiction will remain under EAA jurisdiction.

Representatives of the industry may request semi-annual meetings to request a review of the agreed-upon algorithms and the new procedures. I will host the first such opportunity, which the Software Publishers Association has already requested, in early September.

Attached to this letter is a detailed description of the changes we are making, the text of a note to the relevant regulations (of the International Traffic in Arms Regulations, 22 C.F.R. Section 120.1 et seq.), which is being published in the Federal Register, to reflect these changes, and a letter from the Department of State confirming that they will expeditiously review and transfer to the EAA export control jurisdiction over mass-market software programs with encryption that implement the specified criteria.

This arrangement, we believe, reflects an excellent accommodation of the software publishers' concerns and our need to maintain effective control of this critical technology. The Software Publishers Association agrees that these administrative changes will improve the export licensing process and will obviate the need for the proposed legislation at this time.

Sincerely,


Brent Scowcroft

Attachment

The Honorable Jake Garn
United States Senate
Washington, D.C. 20510

ASSISTANT SECRETARY OF STATE
WASHINGTON

JUL 06 1992

Dear Admiral McConnell:

It is my understanding that, in response to the request of representatives of the mass-market software industry, a process is being established to expedite and improve the predictability of export control procedures applicable to mass-market software with encryption. Requests to the Department of State to transfer the commodity jurisdiction of mass-market software products with encryption designed to meet specified criteria agreed upon by government and industry representatives will be expeditiously reviewed. Technical details as to the criteria, as well as information regarding the procedure, will be available from the Department of State's Office of Defense Trade Controls (DTC).

The following special procedures are being implemented:

-- Commodity jurisdiction requests to transfer commodity jurisdiction of mass-market software that contains encryption for the privacy of data and associated key management that meets the specified known criteria made available by DTC to the industry will be granted on an expedited basis.

-- Information regarding the criteria and procedures will be sent (faxed) to software developers and vendors within one working day of their request to the Department of State's Office of Defense Trade Controls.

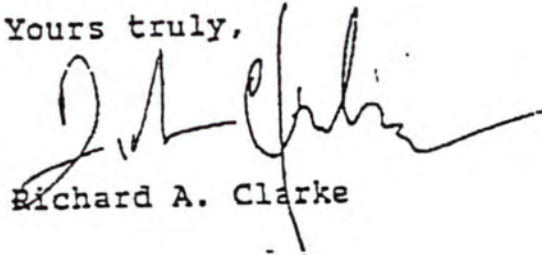
-- The Department of State will, with the cooperation of the National Security Agency and the Departments of Defense and Commerce, expedite the review of such requests, notify the applicant of the transfer or retention of the product, and transfer commodity jurisdiction of verified products to Commerce within seven working days of receipt of a request.

Vice Admiral John McConnell,
Director,
National Security Agency,
Department of Defense,
Washington, D.C.

- 2 -

In this respect, it is my understanding that the National Security Agency will ensure that its own review of software products is completed in a sufficiently timely fashion to allow the Department to undertake this expeditious processing.

Yours truly,

A handwritten signature in dark ink, appearing to read 'R. A. Clarke', with a long horizontal flourish extending to the right.

Richard A. Clarke

DETAILS OF CRITERIA AND PROCEDURES

Specified Criteria

Department of State (DOS) will provide expedited 7-day commodity jurisdiction (CJ) transfers for mass-market software where the data encryption and associated key management functions satisfy the following:

a. Data Encryption (either or both below):

- (i) RC4; 40 bit key (which can vary with every message); with key management as per (b) below or with no key management.

NOTE: It shall be permissible to pre-fix an initialization vector to any plain text message that is to be encrypted with RC4. The initialization vector itself will appear in plain text in the message itself and will be exclusive or'd with the RC4 key prior to RC4 key set up.

- (ii) RC2; 40 bit key; with key management as per (b) below or with no key management

b. Key Management (any or all below):

- (i) key exchange of keys used in data encryption via a public key algorithm which does not exceed 512 bit modulus for the key space; and/or
- (ii) key exchange of keys used in data encryption via symmetric (single key) algorithm (including but not limited to RC2, DES, and proprietary algorithms) with a key space not exceeding 64 bits.

NOTE: use of a public key or symmetric single key algorithms for digital signatures, passwords, access control, and authentication, and associated key management, are unrestricted as to key length size.

Products using only the suite described above for encryption purposes will not be limited to any specific uses for the data encryption; they can be used:

- * for all mass-market applications (e.g. file encryption, network data encryption, disk encryption, etc.), although each different application will be subject to the 7-day CJ process set forth herein;

(3) Requests to transfer commodity jurisdiction or to approve license applications of source code for products approved under paragraphs (1) or (2) above will be approved in 7 working days provided the source code is modified either (a) by deleting the encryption algorithm and its calls, or (b) by providing the encryption algorithm in object code with the calls hidden. Vendors will provide DOS a letter that details how they have met the above provisions, and furnish, in mutually agreeable format, a copy of the sections of the product source code that contain the encryption algorithm and its calls.

Detailed Information To Be Sent To Vendors & Publishers Requesting It

(1) Information regarding the above criteria and procedures will be sent (faxed) to software developers and vendors within one day of their request to DOS Office of Defense Trade Controls.

(2) The information sent by DOS will be that set forth in this Attachment 1.

(3) It will be the responsibility of the individual software developer to contact RSA Data Security, Inc. for details on licensing RC2 and/or RC4 from RSA.

Mass-Market Software Covered By This Proposal

Mass-market software governed by this note is software that is generally available to the public by being --

(i) sold from stock at retail selling points, without restriction, by means of

- (1) over the counter transactions
- (2) mail order transactions, or
- (3) telephone call transactions; and

(ii) designed for installation by the user without further substantial support by the supplier.

NOTE: It is understood that mass-market software subject to these arrangements, once sold, may be distributed from retail selling points by means of over the counter, mail, or telephone transactions. It is also understood that the phrase "substantial support by the supplier" contained in the definition of "mass-market software" does not include telephone help line services (voice only) provided by suppliers for installation or basic operation of the software, or training offered to facilitate the basic operation of installed mass-market software.

Follow-up Discussions

Semi-annually (twice a year), software industry representatives may request, and the government will provide, an opportunity for representatives of the mass-market software industry to present its

concerns about the implementation and suitability of criteria given technological and regulatory developments.

- * The first such opportunity will be hosted by the Assistant to the President for National Security Affairs in early September 1992. The next such opportunity will occur six months after the first one. Beginning with the second opportunity, each such opportunity will be hosted by a representative of the NSC. All discussions between industry and government representatives with regard to industry's presentations will be unclassified.
- * Topics that may be addressed include: implementation of the criteria and procedures set forth herein; continued suitability of the criteria set forth herein including whether the algorithms and/or bit lengths need revision to reflect advances in computing power and speed which facilitate decryption; whether algorithms and/or bit lengths need revision to reflect availability of mass-market software programs with encryption that place U.S. companies at a competitive disadvantage.
- * DOS and DOC representatives will be invited to participate in discussions regarding the transfer of products from the USML to the CCL.

- * in updated versions of the same program. The initial issuance of a program will be subject to the 7-day CJ process set forth herein. Updated versions of programs previously transferred in accordance with the 7-day CJ process, provided that the encryption module is unchanged, will not require CJ transfers.
- * in products and technologies that also employ cryptography for the performance of functions exempted from ITAR controls as set forth in the Final Rule revising, in part, Category XIII of the ITAR which was published in the April 27, 1992 Federal Register (at 15227, 15233). Products using the encryption suite described above will, however, be subject to the CJ process set forth herein.
- * RC4 and RC2 can be used in the same program provided their functionality is kept separate, i.e., no data are operated on by both routines.

Detailed Procedures

(1) For mass-market software programs using only the suite described above, requests to transfer Commodity Jurisdiction shall be granted and faxed to the applicant within seven (7) working days if:

- the vendor completes a key and test vector for the data encryption algorithm and returns the associated cipher text to DOS (with the CJ request) which shows proper implementation, and
- the vendor stipulates that the software has been written to preclude the modification of the key space by users.
- If RC4 and RC2 are used in the same program the vendor will stipulate that there is sufficient separation of their functionality to assure no data are operated on by both routines.

(2) For algorithms and associated key management functions not using the suite described above, requests to transfer Commodity Jurisdiction or requests for license approval will continue to be handled on a case-by-case basis subject to certain time limits:

- Within fifteen (15) working days of the submission of a request for CJ transfer or license approval, the DOS will either: (1) fax the approved license or CJ transfer to the vendor; or (2) contact the vendor and discuss issues about which additional information from the vendor is required.
- Response to the vendor's submission of requested information or a revised program designed to meet DOS objections will be as per above.

DEPARTMENT OF STATE

Bureau of Politico-Military Affairs

22 CFR Part 121

[Public Notice PN 1662]

Amendment to the International Traffic in Arms Regulations (ITAR), the United States Munitions List

AGENCY: Department of State.

ACTION: Interim final rule.

SUMMARY: This rule amends the regulations implementing section 38 of the Arms Export Control Act (AECA). It establishes a process for the expedited movement to the control of the Department of Commerce of mass market software with encryption capabilities which meet certain standards.

EFFECTIVE DATE: This interim final rule is effective immediately.

FOR FURTHER INFORMATION: Details regarding this notice may be obtained from James Andrew Lewis, telephone 202-697-6977 or Daniel L. Cook, telephone 703-875-6647, and details regarding the specified technical characteristics and the expedited commodity jurisdiction process may be obtained from Gary Oncale, Department of State, telephone 703-875-6644.

SUPPLEMENTARY INFORMATION: This rule amends the regulations implementing section 38 of the Arms Export Control Act, which governs the export of defense articles and services. On November 16, 1990, the President signed Executive Order 12735 on Chemical and Biological Weapons Proliferation and directed various other export control measures. The measures directed by the President include the following:

By June 1, 1991, the United States will remove from the U.S. Munitions List all items contained on the COCOM dual-use list unless significant U.S. national security interests would be jeopardized (Memorandum of Disapproval of H.R. 4653, 28 Weekly Compilation of Presidential Documents 1839).

The Department of State published in July, August, and September 1991 notices of proposed rule changes related to the coverage of articles in categories XII, VIII, XX, and XIII. This rule takes

into consideration public comments received in response to these notices. It addresses the request of representatives of the mass-market software industry to relax AECA controls applicable to mass-market software with encryption and to expedite and improve the predictability of procedures to transfer export jurisdiction for such products from the Department of State to the Department of Commerce commodity Control List.

The Department of State has already transferred control of certain mass-marketed software with encryption, when limited to certain functions, to the Department of Commerce (see *Federal Register*, Vol. 57, No. 81/Monday, April 27, 1992/Rules and Regulations, Page 15233 for details). Significant national security interests warrant the continued control of mass-market software products with encryption which can be used to ensure the privacy of data on the U.S. Munitions List. Mass-market software products with encryption that have previously been granted transfers of commodity jurisdiction remain under Department of Commerce jurisdiction. All other such products are under the jurisdiction of the Department of State.

In response to mass-market software industry requests to recognize the particular requirement of that industry for expeditious and predictable export control procedures applicable to mass-market software with encryption, the Department of State has established a process for the expedited review and transfer as appropriate, to the jurisdiction of the Department of Commerce of mass-market software products with encryption that contain certain specified technical characteristics.

Requests to transfer commodity jurisdiction of mass-market software with encryption for privacy of data and the associated key management that meets the specified criteria will be granted on an expedited basis. The Department of State will expeditiously process such a request to verify that the product meets the specified criteria and shall transfer jurisdiction of products so verified to the Department of Commerce.

This amendment involves a foreign affairs function of the United States and is excluded from the major rule

procedures of Executive Order 12291 (46 FR 13193) and the procedures of 5 U.S.C. 553 and 554.

List of Subjects in 22 CFR Part 121

Arms and munitions, Classified information, Exports.

For the reasons set out in the preamble, 22 CFR part 121, § 121.1 is amended to read as follows.

PART 121—THE UNITED STATES MUNITIONS LIST

1. The authority citation for part 121 continues to read as follows:

Authority: Section 38, Pub. L. 90-629, 90 Stat. 744 (22 U.S.C. 2778); E.O. 11958, 42 FR 4311, 3 CFR 1977 Comp. p. 79; 22 U.S.C. 2658.

2. In § 121.1, a note will be added to Category XIII (b)(1) to read as follows:

§ 121.1 General. The United States Munitions List.

• • • • •

Category XIII—Auxiliary Military Equipment

• • • • •

(b) • • •

(1) • • •

Note: A procedure has been established to facilitate the expeditious transfer to the Commodity Control List of mass market software products with encryption that meet specified criteria regarding encryption for the privacy of data and the associated key management. Requests to transfer commodity jurisdiction of mass market software products designed to meet the specified criteria may be submitted in accordance with the commodity jurisdiction provisions of § 120.5. Questions regarding the specified criteria or the commodity jurisdiction process should be addressed to the Office of Defense Trade Controls. All mass market software products with cryptography that were previously granted transfers of commodity jurisdiction will remain under DOC control. Mass market software governed by this note is software that is generally available to the public by being sold from stock at retail selling points, without restriction, by means of over the counter transactions, mail order transactions, or telephone call transactions; and designed for installation by the user without further substantial support by the supplier.

Dated: July 6, 1992.

Richard A. Clarke,

Assistant Secretary of State for Politico-Military Affairs.

[FR Doc. 92-17191 Filed 7-17-92; 9:34 am]

BILLING CODE 4710-25-M



Uses of Cryptography

SCIENTIFIC AMERICAN

AUGUST 1992

\$3.95

Will an American maglev finally fly?

Musical illusions: how pitch tricks the ear.

Encrypted ID's for digital privacy.



Restless Kilauea: understanding its dynamic processes helps to predict other volcanic eruptions.

Achieving Electronic Privacy

A cryptographic invention known as a blind signature permits numbers to serve as electronic cash or to replace conventional identification. The author hopes it may return control of personal information to the individual

by David Chaum

Every time you make a telephone call, purchase goods using a credit card, subscribe to a magazine or pay your taxes, that information goes into a data base somewhere. Furthermore, all these records can be linked so that they constitute in effect a single dossier on your life—not only your medical and financial history but also what you buy, where you travel and whom you communicate with. It is almost impossible to learn the full extent of the files that various organizations keep on you, much less to assure their accuracy or to control who may gain access to them.

Organizations link records from different sources for their own protection. Certainly it is in the interest of a bank looking at a loan application to know that John Doe has defaulted on four similar loans in the past two years. The bank's possession of that information also helps its other customers, to whom the bank passes on the cost of bad loans. In addition, these records permit Jane Roe, whose payment history is impeccable, to establish a charge account at a shop that has never seen her before.

That same information in the wrong hands, however, provides neither protection for businesses nor better service for consumers. Thieves routinely use a stolen credit card number to trade on their victims' good payment records;

murderers have tracked down their targets by consulting government-maintained address records. On another level, the U.S. Internal Revenue Service has attempted to single out taxpayers for audits based on estimates of household income compiled by mailing-list companies.

The growing amounts of information that different organizations collect about a person can be linked because all of them use the same key—in the U.S. the social security number—to identify the individual in question. This identifier-based approach perforce trades off security against individual liberties. The more information that organizations have (whether the intent is to protect them from fraud or simply to target marketing efforts), the less privacy and control people retain.

Over the past eight years, my colleagues and I at CWI (the Dutch nationally funded Center for Mathematics and Computer Science in Amsterdam) have developed a new approach, based on fundamental theoretical and practical advances in cryptography, that makes this trade-off unnecessary. Transactions employing these techniques avoid the possibility of fraud while maintaining the privacy of those who use them.

In our system, people would in effect give a different (but definitively verifiable) pseudonym to every organization they do business with and so make dossiers impossible. They could pay for goods in untraceable electronic cash or present digital credentials that serve the function of a banking passbook, driver's license or voter registration card without revealing their identity. At the same time, organizations would benefit from increased security and lower record-keeping costs.

Recent innovations in microelectronics make this vision practical by providing personal "representatives" that store and manage their owners' pseudonyms, credentials and cash. Micropro-

cessors capable of carrying out the necessary algorithms have already been embedded in pocket computers the size and thickness of a credit card. Such systems have been tested on a small scale and could be in widespread use by the middle of this decade.

The starting point for this approach is the digital signature, first proposed in 1976 by Whitfield Diffie, then at Stanford University. A digital signature transforms the message that is signed so that anyone who reads it can be sure of who sent it [see "The Mathematics of Public-Key Cryptography," by Martin E. Hellman; *SCIENTIFIC AMERICAN*, August 1979]. These signatures employ a secret key used to sign messages and a public one used to verify them. Only a message signed with the private key can be verified by means of the public one. Thus, if Alice wants to send a signed message to Bob (these two are the cryptographic community's favorite hypothetical characters), she transforms it using her private key, and he applies her public key to make sure that it was she who sent it. The best methods known for producing forged signatures would require many years, even using computers billions of times faster than those now available.

To see how digital signatures can provide all manner of unforgeable credentials and other services, consider how they might be used to provide an electronic replacement for cash. The First Digital Bank would offer electronic bank notes: messages signed using a particular private key. All messages bearing one key might be worth a dollar, all those bearing a different key five dollars, and so on for whatever denominations were needed. These electronic bank notes could be authenticated using the corresponding public key, which the bank has made a matter of record. First Digital would also make public a key to authenticate electronic documents

DAVID CHAUM is head of the Cryptography Group at the Center for Mathematics and Computer Science (CWI) in Amsterdam. He is also a founder of Digi-Cash, which develops electronic payment systems. Chaum received his Ph.D. in computer science from the University of California, Berkeley, in 1982 and joined CWI in 1984. He helped to found the International Association for Cryptologic Research and remains active on its board; he also consults internationally on cryptology.

sent from the bank to its customers.

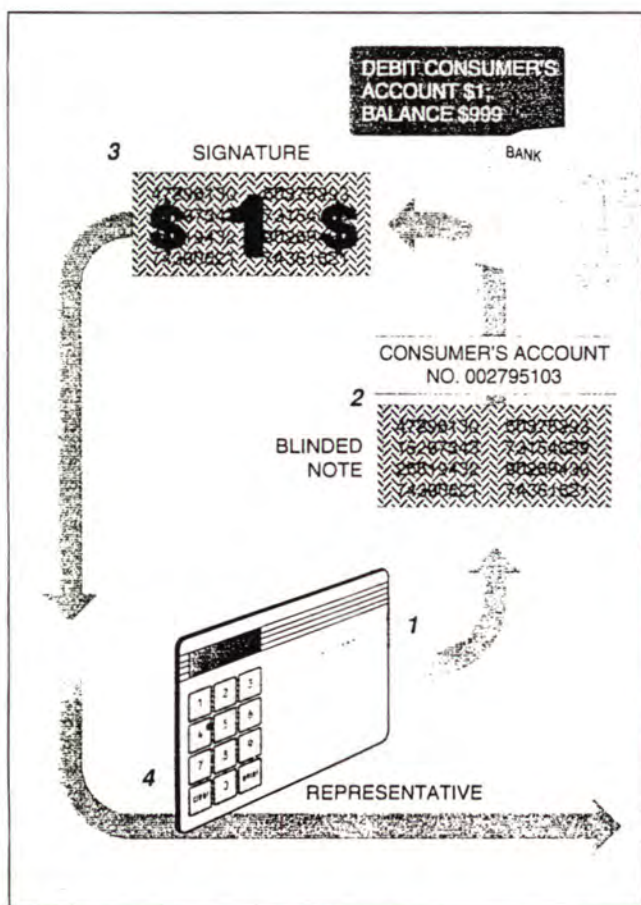
To withdraw a dollar from the bank, Alice generates a note number (each note bears a different number, akin to the serial number on a bill); she chooses a 100-digit number at random so that the chance anyone else would generate the same one is negligible. She signs the number with the private key corresponding to her "digital pseudonym" (the public key that she has previously established for use with her account). The bank verifies Alice's signature and removes it from the note number, signs the note number with its worth-one-dollar signature and debits her account. It then returns the signed note along with a digitally signed withdrawal receipt for Alice's records. In practice, the creation, signing and transfer of note numbers would be carried out by Alice's card computer. The power of the cryptographic protocols, however, lies in the fact that they are secure regardless of physical medium: the same transactions could be carried out using only pencil and paper.

When Alice wants to pay for a purchase at Bob's shop, she connects her "smart" card with his card reader and transfers one of the signed note numbers the bank has given her. After verifying the bank's digital signature, Bob transmits the note to the bank, much as a merchant verifies a credit card transaction today. The bank re-verifies its signature, checks the note against a list of those already spent and credits Bob's account. It then transmits a "deposit slip," once again unforgeably signed with the appropriate key. Bob hands the merchandise to Alice along with his own digitally signed receipt, completing the transaction.

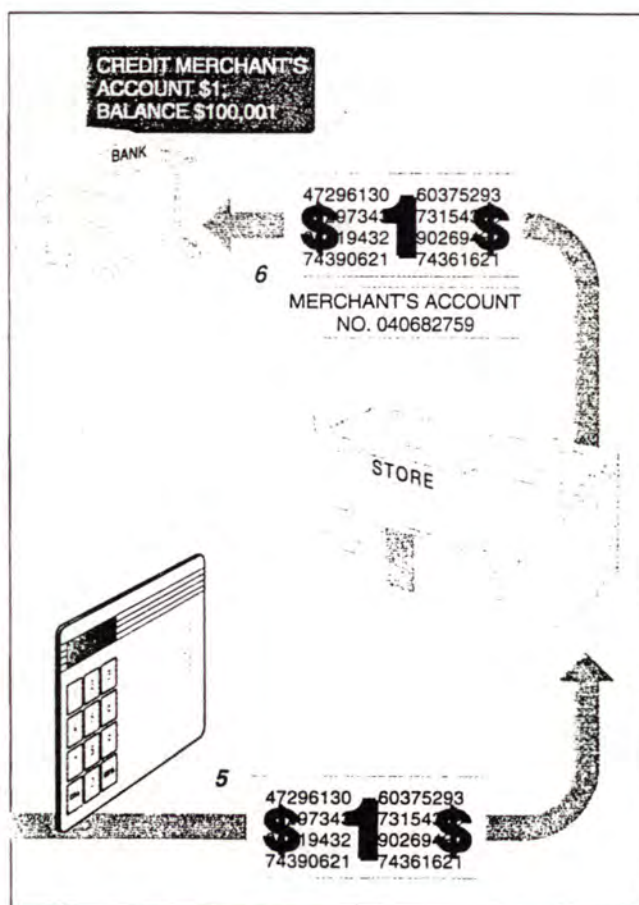
This system provides security for all three parties. The signatures at each stage prevent any one from cheating either of the others: the shop cannot deny that it received payment, the bank cannot deny that it issued the notes or that it accepted them from the shop for deposit, and the customer can neither deny withdrawing the notes from her account nor spend them twice.

This system is secure, but it has no privacy. If the bank keeps track of note numbers, it can link each shop's deposit to the corresponding withdrawal and so determine precisely where and when Alice (or any other account holder) spends her money. The resulting dossier is far more intrusive than those now being compiled. Furthermore, records based on digital signatures are more vulnerable to abuse than conventional files. Not only are they self-authenticating (even if they are copied, the information they contain can be verified by anyone), but they also permit a person who has a particular kind of information to prove its existence without either giving the information away or revealing its source. For example, someone might be able to prove incontrovertibly that Bob had telephoned Alice on 12 separate occasions without having to reveal the time and place of any of the calls.

I have developed an extension of digital signatures, called blind signatures, that can restore privacy. Before send-

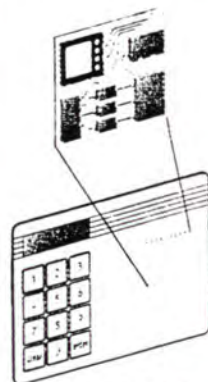


DIGITAL CASH flows tracelessly from bank through consumer and merchant before returning to the bank. Using a small computer "representative," a person creates a random number to serve as a bank note. The bank debits the appropriate account and signs the note with an unforgeable digital

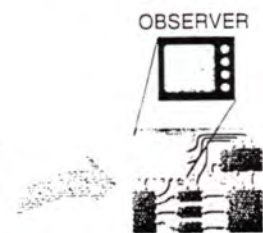


signature indicating its value. The bank credits the merchant's account when the note is presented for payment. A technique known as a blind signature prevents the bank from seeing the note number so the bank will be unable to correlate withdrawals from one account with deposits to another.

How to Create Secure Digital Pseudonyms



REPRESENTATIVE

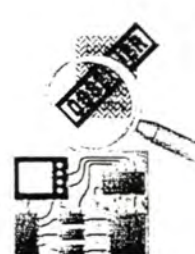


Each personal representative contains an embedded observer in addition to its own microprocessor.



The representative and the observer generate numbers that the observer uses to produce a set of blinded digital pseudonyms.

The observer signs the pseudonyms with a special built-in key.



The representative checks the pseudonyms to make sure they do not disclose any illicit information and passes them to a validating authority.

ing a note number to the bank for signing, Alice in essence multiplies it by a random factor. Consequently, the bank knows nothing about what it is signing except that it carries Alice's digital signature. After receiving the blinded note signed by the bank, Alice divides out the blinding factor and uses the note as before.

The blinded note numbers are "unconditionally untraceable"—that is, even if the shop and the bank collude, they cannot determine who spent which notes. Because the bank has no idea of the blinding factor, it has no way of linking the note numbers that Bob deposits with Alice's withdrawals. Whereas the security of digital signatures is dependent on the difficulty of particular computations, the anonymity of blinded notes is limited only by the unpredictability of Alice's random numbers. If she wishes, however, Alice can reveal these numbers and permit the notes to be stopped or traced.

Blinded electronic bank notes protect an individual's privacy, but because each note is simply a number, it can be copied easily. To prevent double spending, each note must be checked on-line against a central list when it is spent. Such a verification procedure might be acceptable when large amounts of money are at stake, but it is far too expensive to use when someone is just buying a newspaper. To solve this problem, my colleagues Amos Fiat and Moni Naor and I have proposed a method for generating blinded notes that requires the payer to answer a random numeric query about each note when making a payment. Spending such a note once does not compromise unconditional untrace-

ability, but spending it twice reveals enough information to make the payer's account easily traceable. In fact, it can yield a digitally signed confession that cannot be forged even by the bank.

Cards capable of such anonymous payments already exist. Indeed, Digi-Cash, a company with which I am associated, has installed equipment in two office buildings in Amsterdam that permits copiers, fax machines, cafeteria cash registers and even coffee vending machines to accept digital "bank notes." We have also demonstrated a system for automatic toll collection in which automobiles carry a card that responds to radioed requests for payment even as they are traveling at highway speeds.

My colleagues and I call a computer that handles such cryptographic transactions a "representative." A person might use different computers as representatives depending on which was convenient: Bob might purchase software (transmitted to him over a network) by using his home computer to produce the requisite digital signatures, go shopping with a "palm-top" personal computer and carry a smart credit card to the beach to pay for a drink or crab cakes. Any of these machines could represent Bob in a transaction as long as the digital signatures each generates are under his control.

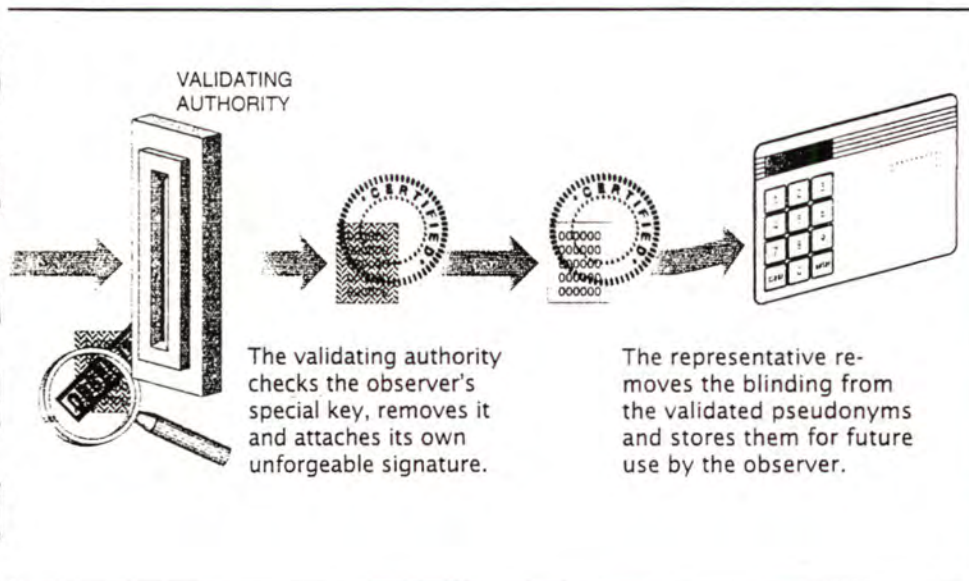
Indeed, such computers can act as representatives for their owners in virtually any kind of transaction. Bob can trust his representative and Alice hers because they have each chosen their own machine and can reprogram it

at will (or, in principle, build it from scratch). Organizations are protected by the cryptographic protocol and so do not have to trust the representatives.

The prototypical representative is a smart credit-card-size computer containing memory and a microprocessor. It also incorporates its own keypad and display so that its owner can control the data that are stored and exchanged. If a shop provided the keypad and display, it could intercept passwords on their way to the card or show one price to the customer and another to the card. Ideally, the card would communicate with terminals in banks and shops by a short-range communications link such as an infrared transceiver and so need never leave its owner's hands.

When asked to make a payment, the representative would present a summary of the particulars and await approval before releasing funds. It would also insist on electronic receipts from organizations at each stage of all transactions to substantiate its owner's position in case of dispute. By requiring a password akin to the PIN (personal identifying number) now used for bank cards, the representative could safeguard itself from abuse by thieves. Indeed, most people would probably keep backup copies of their keys, electronic bank notes and other data; they could recover their funds if a representative were lost or stolen.

Personal representatives offer excellent protection for individual privacy, but organizations might prefer a mechanism to protect their interests as strongly as possible. For example, a bank might want to prevent double spending of bank notes altogether rather than



simply detecting it after the fact. Some organizations might also want to ensure that certain digital signatures are not copied and widely disseminated (even though the copying could be detected afterward).

Organizations have already begun issuing tamperproof cards (in effect, their own representatives) programmed to prevent undesirable behavior. But these cards can act as "Little Brothers" in everyone's pocket.

We have developed a system that satisfies both sides. An observer—a tamper-resistant computer chip, issued by some entity that organizations can trust—acts like a notary and certifies the behavior of a representative in which it is embedded. Philips Industries has recently introduced a tamper-resistant chip that has enough computing power to generate and verify digital signatures. Since then, Siemens, Thomson CSF and Motorola have announced plans for similar circuits, any of which could easily serve as an observer.

The central idea behind the protocol for observers is that the observer does not trust the representative in which it resides, nor does the representative trust the observer. Indeed, the representative must be able to control all data passing to or from the observer; otherwise the tamperproof chip might be able to leak information to the world at large.

When Alice first acquires an observer, she places it in her smart-card representative and takes it to a validating authority. The observer generates a batch of public and private key pairs from a combination of its own random numbers and numbers supplied by the

card. The observer does not reveal its numbers but reveals enough information about them so that the card can later check whether its numbers were in fact used to produce the resulting keys. The card also produces random data that the observer will use to blind each key.

Then the observer blinds the public keys, signs them with a special built-in key and gives them to the card. The card verifies the blinding and the signature and checks the keys to make sure they were correctly generated. It passes the blinded, signed keys to the validating authority, which recognizes the observer's built-in signature, removes it and signs the blinded keys with its own key. The authority passes the keys back to the card, which unblinds them. These keys, bearing the signature of the validating authority, serve as digital pseudonyms for future transactions; Alice can draw on them as needed.

An observer could easily prevent (rather than merely detect) double spending of electronic bank notes. When Alice withdraws money from her bank, the observer witnesses the process and so knows what notes she received. At Bob's shop, when Alice hands over a note from the bank, she also hands over a digital pseudonym (which she need use only once) signed by the validating authority. Then the observer, using the secret key corresponding to the validated pseudonym, signs a statement certifying that the note will be spent only once, at Bob's shop and at this particular time and date. Alice's card verifies the signed statement to make sure that the observer does not

leak any information and passes it to Bob. The observer is programmed to sign only one such statement for any given note.

Many transactions do not simply require a transfer of money. Instead they involve credentials—information about an individual's relationship to some organization. In today's identifier-based world, all of a person's credentials are easily linked. If Alice is deciding whether to sell Bob insurance, for example, she can use his name and date of birth to gain access to his credit status, medical records, motor vehicle file and criminal record, if any.

Using a representative, however, Bob would establish relationships with different organizations under different digital pseudonyms. Each of them can recognize him unambiguously, but none of their records can be linked.

In order to be of use, a digital credential must serve the same function as a paper-based credential such as a driver's license or a credit report. It must convince someone that the person attached to it stands in a particular relation to some issuing authority. The name, photograph, address, physical description and code number on a driver's license, for example, serve merely to link it to a particular person and to the corresponding record in a data base. Just as a bank can issue unforgeable, untraceable electronic cash, so too could a university issue signed digital diplomas or a credit-reporting bureau issue signatures indicating a person's ability to repay a loan.

When the young Bob graduates with honors in medieval literature, for example, the university registrar gives his representative a digitally signed message asserting his academic credentials. When Bob applies to graduate school, however, he does not show the admissions committee that message. Instead his representative asks its observer to sign a statement that he has a B.A. cum laude and that he qualifies for financial aid based on at least one of the university's criteria (but without revealing which ones). The observer, which has verified and stored each of Bob's credentials as they come in, simply checks its memory and signs the statement if it is true.

In addition to answering just the right question and being more reliable than paper ones, digital credentials would be both easier for individuals to obtain and to show and cheaper for organizations to issue and to authenticate. People would no longer need to fill out long and revealing forms. In-

stead their representatives would convince organizations that they meet particular requirements without disclosing any more than the simple fact of qualification. Because such credentials reveal no unnecessary information, people would be willing to use them even in contexts where they would not willingly show identification, thus enhancing security and giving the organization more useful data than it would otherwise acquire.

Positive credentials, however, are not the only kind that people acquire. They may also acquire negative credentials, which they would prefer to conceal: felony convictions, license suspensions or statements of pending bankruptcy. In many cases, individuals will give organizations the right to inflict negative credentials on them in return for some service. For instance, when Alice borrows books from a library, her observer would be instructed to register an overdue notice unless it had received a receipt for the books' return within some fixed time.

Once the observer has registered a negative credential, an organization can find out about it simply by asking the observer (through the representative) to sign a message attesting to its presence or absence. Although a representative could muzzle the observer, it could not forge an assertion about the state of its credentials. In other cases, organizations

might simply take the lack of a positive credential as a negative one. If Bob signs up for skydiving lessons, his instructors may assume that he is medically unfit unless they see a credential to the contrary.

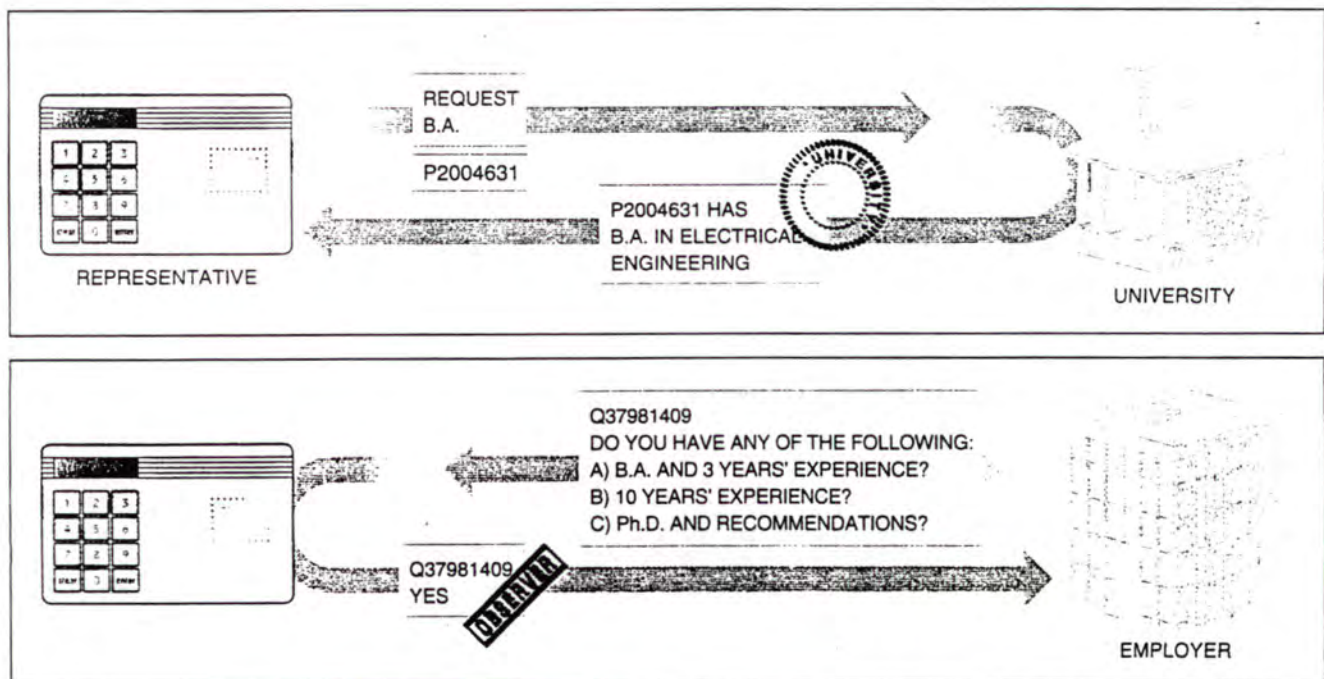
For most credentials, the digital signature of an observer is sufficient to convince anyone of its authenticity. Under some circumstances, however, an organization might insist that an observer demonstrate its physical presence. Otherwise, for example, any number of people might be able to gain access to nontransferable credentials (perhaps a health club membership) by using representatives connected by concealed communications links to another representative containing the desired credential.

Moreover, the observer must carry out this persuasion while its input and output are under the control of the representative that contains it. When Alice arrives at her gym, the card reader at the door sends her observer a series of single-bit challenges. The observer immediately responds to each challenge with a random bit that is encoded by the card on its way back to the organization. The speed of the observer's response establishes that it is inside the card (since processing a single bit introduces almost no delay compared with the time that signals take to traverse a wire). After a few dozen iter-

ations the card reveals to the observer how it encoded the responses; the observer signs a statement including the challenges and encoded responses only if it has been a party to that challenge-response sequence. This process convinces the organization of the observer's presence without allowing the observer to leak information.

Organizations can also issue credentials using methods that depend on cryptography alone rather than on observers. Although currently practical approaches can handle only relatively simple queries, Gilles Brassard of the University of Montreal, Claude Crépeau of the École Normale Supérieure and I have shown how to answer arbitrary combinations of questions about even the most complex credentials while maintaining unconditional unlinkability. The concealment of purely cryptographic negative credentials could be detected by the same kinds of techniques that detect double spending of electronic bank notes. And a combination of these cryptographic methods with observers would offer accountability after the fact even if the observer chip were somehow compromised.

The improved security and privacy of digital pseudonyms exact a price: responsibility. At present, for example, people can disavow credit card purchases made over the tele-



DIGITAL CREDENTIALS put personal information under the control of an individual's representative and its observer. When Alice (one of the author's two hypothetical characters) finishes her undergraduate work, the university gives

her a digitally signed degree. Later, her observer can use its knowledge of the degree to answer questions about her qualifications without revealing any more information about her than absolutely necessary.

phone or cash withdrawals from an automatic teller machine (ATM). The burden of proof is on the bank to show that no one else could have made the purchase or withdrawal. If computerized representatives become widespread, owners will establish all their own passwords and so control access to their representatives. They will be unable to disavow a representative's actions.

Current tamper-resistant systems such as ATMs and their associated cards typically rely on weak, inflexible security procedures because they must be used by people who are neither highly competent nor overly concerned about security. If people supply their own representatives, they can program them for varying levels of security as they see fit. (Those who wish to trust their assets to a single four-digit code are free to do so, of course.) Bob might use a short PIN (or none at all) to authorize minor transactions and a longer password for major ones. To protect himself from a robber who might force him to give up his passwords at gunpoint, he could use a "duress code" that would cause the card to appear to operate normally while hiding its more important assets or credentials or perhaps alerting the authorities that it had been stolen.

A personal representative could also recognize its owner by methods that most people would consider unreasonably intrusive in an identifier-based system; a notebook computer, for example, might verify its owner's voice or even fingerprints. A supermarket check-out scanner capable of recognizing a person's thumbprint and debiting the cost of groceries from their savings account is Orwellian at best. In contrast, a smart credit card that knows its owner's touch and does out electronic bank notes is both anonymous and safer than cash. In addition, incorporating some essential part of such identification technology into the tamper-proof observer would make such a card suitable even for very high security applications.

Computerized transactions of all kinds are becoming ever more pervasive. More than half a dozen countries have developed or are testing chip cards that would replace cash. In Denmark, a consortium of banking, utility and transport companies has announced a card that would replace coins and small bills; in France, the telecommunications authorities have proposed general use of the smart cards now used at pay telephones. The government of Singapore has requested



COMPUTERIZED CREDIT CARD developed by Toshiba and Visa International contains a microprocessor, memory, keypad and display. Although this card identifies its user during transactions, the same hardware could be reprogrammed as a personal representative for spending digital cash.

bids for a system that would communicate with cars and charge their smart cards as they pass various points on a road (as opposed to the simple vehicle identification systems already in use in the U.S. and elsewhere). And cable and satellite broadcasters are experimenting with smart cards for delivering pay-per-view television. All these systems, however, are based on cards that identify themselves during every transaction.

If the trend toward identifier-based smart cards continues, personal privacy will be increasingly eroded. But in this conflict between organizational security and individual liberty, neither side emerges as a clear winner. Each round of improved identification techniques, sophisticated data analysis or extended linking can be frustrated by widespread noncompliance or even legislated limits, which in turn may engender attempts at further control.

Meanwhile, in a system based on representatives and observers, organizations stand to gain competitive and political advantages from increased public confidence (in addition to the lower costs of pseudonymous record-keeping). And individuals, by maintaining their own cryptographically guaranteed records and making only necessary disclosures, will be able to protect their privacy without infringing on the legiti-

mate needs of those with whom they do business.

The choice between keeping information in the hands of individuals or of organizations is being made each time any government or business decides to automate another set of transactions. In one direction lies unprecedented scrutiny and control of people's lives, in the other, secure parity between individuals and organizations. The shape of society in the next century may depend on which approach predominates.

FURTHER READING

- SECURITY WITHOUT IDENTIFICATION: TRANSACTION SYSTEMS TO MAKE BIG BROTHER OBSOLETE. David Chaum in *Communications of the ACM*, Vol. 28, No. 10, pages 1030-1044; October 1985.
- THE DINING CRYPTOGRAPHERS PROBLEM: UNCONDITIONAL SENDER AND RECIPIENT UNTRACEABILITY. David Chaum in *Journal of Cryptology*, Vol. 1, No. 1, pages 65-75; 1988.
- MODERN CRYPTOLOGY: A TUTORIAL. Gilles Brassard in *Lecture Notes in Computer Science*, Vol. 325. Springer-Verlag, 1988.
- PRIVACY PROTECTED PAYMENTS: UNCONDITIONAL PAYER AND/OR PAYEE UNTRACEABILITY. David Chaum in *Smart Card 2000: The Future of IC Cards*. Edited by David Chaum and Ingrid Schauer-müller-Bichl. North-Holland, 1989.

INTERNET PRIVACY ENHANCED MAIL (PEM)

Stephen Crocker

Trusted Information Systems
3060 Washington Road (Rt. 97)
Glenwood, Maryland 21738
(301) 854-6889
FAX (301) 854-5363

crocker@tis.com



WHAT IS PRIVACY ENHANCED MAIL?

SIMPLE SECURITY SERVICES

- Message integrity
- Sender authentication (w/ non-repudiation)
- Message confidentiality

ADDED TO REGULAR ELECTRONIC MAIL

- RFC 822
- UA-to-UA protection
- Independent of MTA and lower layers

EXAMPLE SIGNED MESSAGE

To: Steve Crocker <crocker@TIS.COM>, Jim Galvin <galvin@TIS.COM>
Cc: David M Balenson <balenson@TIS.COM>
Subject: Example MIC-CLEAR message
Date: Mon, 01 Feb 93 15:09:17 -0500
From: "David M. Balenson" <balenson@TIS.COM>

-----BEGIN PRIVACY-ENHANCED MESSAGE-----

Proc-Type: 4,MIC-CLEAR

Content-Domain: RFC822

Originator-ID-Asymmetric: MEYxCzAJBgNVBAYTA1VTMSQwIgYDVQQKEExtUcnV
zdGVkIEluZm9ybWFOaW9uIFN5c3RlbXMxETAPBgNVBAsTCEDsZW53b29k,14

MIC-Info: RSA-MD5,RSA,je8ccRcyNzoebxXbtCVxPdXTMYmQeUo7cHNq4FcM8+B
MqOilTpq9/LdnYXP6SRfJg+0ijdo/L7o1nqSxA7/QpQ==

This is an example MIC-CLEAR message.

- -DB

-----END PRIVACY-ENHANCED MESSAGE-----

EXAMPLE MIC-ONLY MESSAGE

To: Steve Crocker <crocker@TIS.COM>, Jim Galvin <galvin@TIS.COM>
Cc: David M Balenson <balenson@TIS.COM>
Subject: Example MIC-ONLY message
Date: Tue, 19 Jan 93 16:13:28 -0500
From: "David M. Balenson" <balenson@TIS.COM>

-----BEGIN PRIVACY-ENHANCED MESSAGE-----

Proc-Type: 4,MIC-ONLY

Content-Domain: RFC822

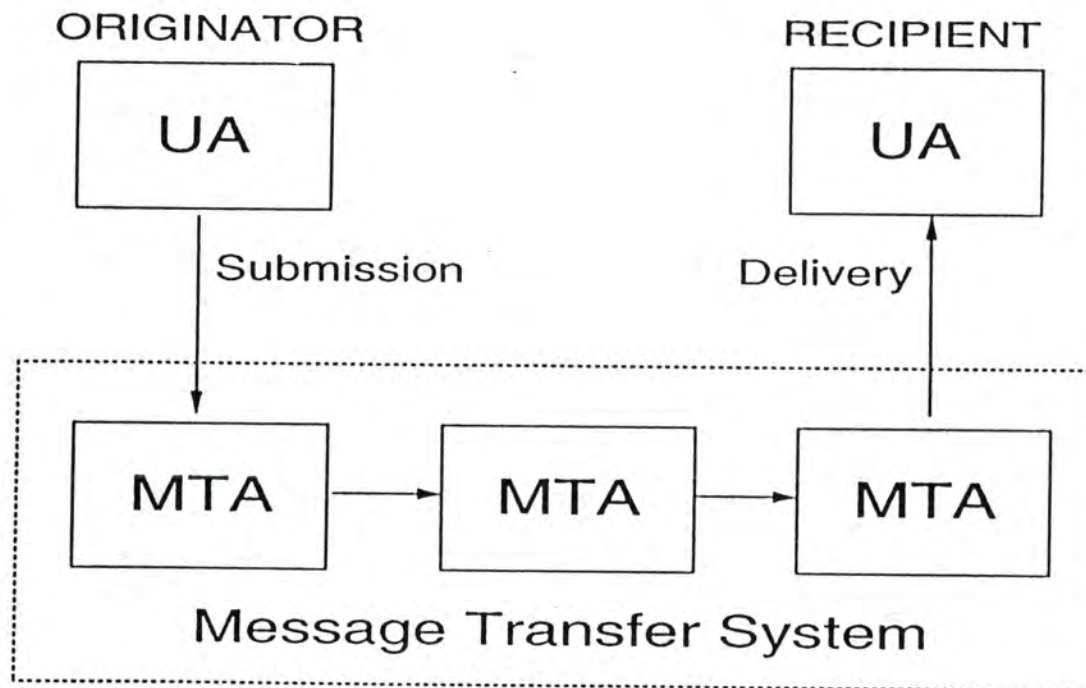
Originator-ID-Asymmetric: MEYxCzAJBgNVBAYTA1VTMSQwIgYDVQQKEExtUcnV
zdGVkIEluZm9ybW90aW9uIFN5c3RlbXMxETAPBgNVBAsTCEDsZW53b29k,14

MIC-Info: RSA-MD5,RSA,dPhpOyWQZJRDaVsQUpPsURjcEcmgXdm0GV6zduAKs6S
3O23d4SHIcjVbpbZ3SLevsjbaieViiWrr8a8/pLZ7dA==

VGhpcyBpcyBhbiBleGFtcGxlIE1JQy1PTkxZIG1lc3NhZ2UuDQoNCi1EQg0KDQo=

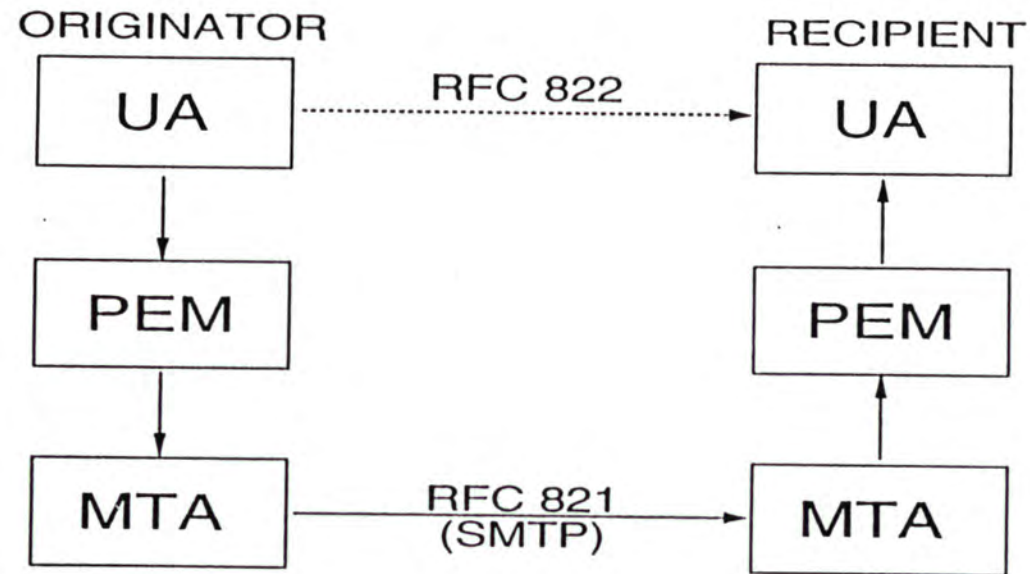
-----END PRIVACY-ENHANCED MESSAGE-----

MESSAGE HANDLING SYSTEM (MHS) MODEL



UA - User Agent
MTA - Message Transfer Agent

INTERNET MAIL AND PEM



UA - User Agent

MTA - Message Transfer Agent (e.g., sendmail, MMDF II)

PEM - Privacy Enhanced Mail

TWO TYPES OF MESSAGES

- SIGNED

Signed to ensure authenticity of sender and integrity of message contents

- MIC-CLEAR

- MIC-ONLY

- ENCRYPTED

Signed (as above) and encrypted to ensure confidentiality of message contents



PEM TECHNOLOGIES

CRYPTOGRAPHY

- Sensitive But Unclassified Use

CERTIFICATES

- Key management based on CCITT Recommendation X.509
"The Directory - Authentication Framework"



PEM CRYPTOGRAPHIC ALGORITHMS

<i>Mechanism/ Security Service</i>	<i>Algorithms</i>
Message Hash (Message Integrity)	MD2 or MD5
Message Encryption (Message Confidentiality)	DES
Digital Signature	RSA
Key Management	RSA

ALTERNATIVE CRYPTOGRAPHIC ALGORITHMS

<u>Mechanism/ Security Service</u>	<u>Algorithms</u>		
	<u>PEM</u>	<u>INT'L?</u>	<u>MOSAIC (PMSP)</u>
Message Hash (Message Integrity)	MD2 MD5	MD2 MD5	SHA
Message Encryption (Message Confidentiality)	DES	RC2/40	SKIPJACK
Digital Signature	RSA	RSA	DSA
Key Management	RSA	RSA/512	"KEA"

PUBLIC KEYS AND USER IDENTITIES

- User keeps private key hidden
- Public key is made available to others
 - direct access
 - directories
- Need a mechanism for assuring relationship between public key and user

A SAMPLE CERTIFICATE

Distinguished Name:

John P. Doe, Avuncular Technologies, Inc.
123 SoftSell Lane, Cotton, Texas

Public Key: RSA, EF29A789BE5632730681

Serial Number: 068305

Validity Period: 031792-031794

Certified By: Great SouthWest PCA

Signature: MD2, RSA, 9373AB81ED932A90

CERTIFICATE

- Binds user identification to public key
- Adequate description of user, e.g., name, employer, position, home address
- Certificate must be guaranteed by Issuing Authority
- Issuing Authority must have a certificate ...
- Common root or cross-certification required

EXAMPLE MIC-CLEAR MESSAGE (With Originator Certificate)

To: Steve Crocker <crocker@TIS.COM>, Jim Galvin <galvin@TIS.COM>
Cc: David M Balenson <balenson@TIS.COM>
Subject: Example MIC-CLEAR message (with originator certificate)
Date: Mon, 01 Feb 93 15:09:23 -0500
From: "David M. Balenson" <balenson@TIS.COM>

-----BEGIN PRIVACY-ENHANCED MESSAGE-----

Proc-Type: 4,MIC-CLEAR

Content-Domain: RFC822

Originator-Certificate: MIIBkDCCAToCARQwDQYJKoZIhvcNAQECBQAwRjELM
AkGA1UEBhMCVVMxJDAiBgNVBAoTG1RydXN0ZWQgSW5mb3JtYXRpb24gU3lzdGVtc
zERMA8GA1UECzMIR2xlbndvb2QwHhcNOTIwNzIwMTkwNTE3WhcNOTQwNzIwMTkwN
TE3WjBiMQswCQYDVQQGEwJVUzEkMCIGA1UEChMbVHJ1c3RlZCBJbmZvcmlhdGlvb
iBTeXN0ZW1zMREwDwYDVQQLEwhHbGVud29vZDEaMBGGA1UEAxMRRGF2aWQgTS4gQ
mFsZW5zb24wWjANBgkqhkiG9w0BAQEFAANJADBGAkEAWCrBNW5Hz9TxYchod+ujL
4aT7x3KP8UIywfpYYSZUBC0/WYloH0W1ymDuNtsQZ0Xp35pvpSTnWyMO3rU/t6Nfe
wIBAzANBgkqhkiG9w0BAQIFAANBAI7DbnrwjTGcpRARWgYUQDAXgGJvF+zv1OIkJ
BJnPRBDYjTffTHNjDJM+VbwHcqY5SRxyMX+BzUBS8Kh1uOGkctc=

MIC-Info: RSA-MD5, RSA, je8ccRcyNzoebxXbtCvXpDXTMYmQeUo7cHN4FcM8+B
MqOilTpq9/LdnYXP6SRfJg+0ijdo/L7o1nqsxA7/QpQ==

This is an example MIC-CLEAR message.

- -DB

-----END PRIVACY-ENHANCED MESSAGE-----

EXAMPLE ENCRYPTED MESSAGE

To: Steve Crocker <crocker@TIS.COM>, Jim Galvin <galvin@TIS.COM>
Cc: David M Balenson <balenson@TIS.COM>
Subject: Example ENCRYPTED message
Date: Tue, 19 Jan 93 16:14:57 -0500
From: "David M. Balenson" <balenson@TIS.COM>

-----BEGIN PRIVACY-ENHANCED MESSAGE-----

Proc-Type: 4, ENCRYPTED

Content-Domain: RFC822

DEK-Info: DES-CBC, 941F8C8ADE2AC0B9

Originator-ID-Asymmetric: MEYxCzAJBgNVBAYTA1VTMSQwIgYDVQQKEExtUcnV
zdGVkIEluZm9ybWFOaW9uIFN5c3RlbXMxETAPBgNVBAsTCEdsZW53b29k, 14

Key-Info: RSA, YiCP4GseUMPM0BGj4bAsaZFnpzhlmLjzlaNIUT8uJwSYvR0lnh
003H/0iQvUxZqtaYDhMOJBFadhMVCZSSUHA==

MIC-Info: RSA-MD5, RSA, 0gZwOc2mNhzoFhe6/Be7r4JR9qaQ4j+q8/Y7+0+7qfo
E5TN3u2ggs22pNVyQrxfr5ORdtPNrKO0qe1+LWGACGONz1Q1SzMoY

Recipient-ID-Asymmetric: MEYxCzAJBgNVBAYTA1VTMSQwIgYDVQQKEExtUcnVz
dGVkIEluZm9ybWFOaW9uIFN5c3RlbXMxETAPBgNVBAsTCEdsZW53b29k, 0F

Key-Info: RSA, DDdkni3BU0RSM0uLXWEkOscFEr63rjMXeMmxe5eBHJSBkvNLVt
lDCFX7FhnDwcUlle0VkcD2Sb/PROkcKAM0A==

Recipient-ID-Asymmetric: MEYxCzAJBgNVBAYTA1VTMSQwIgYDVQQKEExtUcnVz
dGVkIEluZm9ybWFOaW9uIFN5c3RlbXMxETAPBgNVBAsTCEdsZW53b29k, 02

Key-Info: RSA, wwsTMOfcvVy12S2HWKoheZNQPhexXMg90FVpXfFiU6ArJIogVUJ
L0X3DT7jbw8Pz854BdqW8GVjMImU4awQVRA==

Iu/QMWdHp+JS3hODjynck4iZ6I1az2n/c5T9ah6XfYzNiGEFmWOUqWginiz4n7EG
jEE6lPJNGKQ=

-----END PRIVACY-ENHANCED MESSAGE-----



CERTIFICATION AUTHORITIES

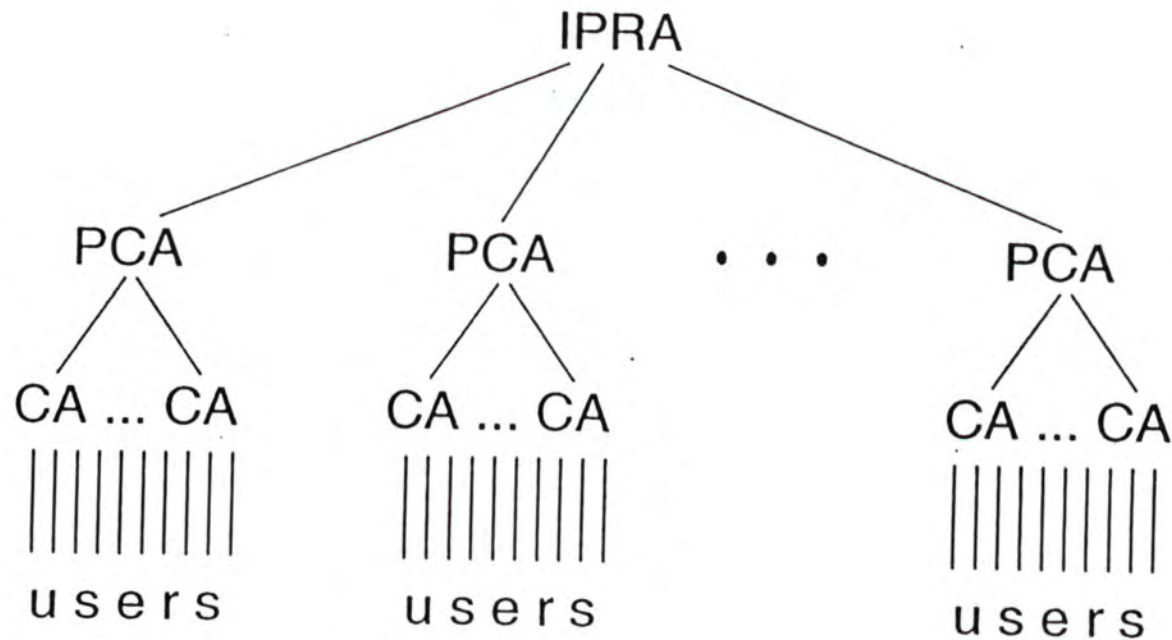
- "An authority trusted by one or more users to create and assign certificates." (X.509)
- In the PEM environment the certification hierarchy is very closely tied to the naming hierarchy
- In the PEM environment there will be three types of certification authorities:
 - Internet PCA Registration Authority (IPRA)
 - Policy Certification Authorities (PCAs)
 - Certification Authorities (CAs)

CERTIFICATION AUTHORITY

- Must register with PCA and pay fees
- Administers issuance and revocation of user certificates



INTERNET CERTIFICATION HIERARCHY



Phil's Pretty Good Software
Presents

==
PGP
==

Pretty Good Privacy
Public Key Encryption for the Masses

PGP User's Guide
Volume I: Essential Topics

by Philip Zimmermann
Revised 6 Mar 93

PGP Version 2.2 - 6 Mar 93
Software by
Philip Zimmermann
with
Branko Lankester, Hal Finney, and Peter Gutmann

Synopsis: PGP uses public-key encryption to protect E-mail and data files. Communicate securely with people you've never met, with no secure channels needed for prior exchange of keys. PGP is well featured and fast, with sophisticated key management, digital signatures, data compression, and good ergonomic design.

Software and documentation (c) Copyright 1990-1992 Philip Zimmermann. For information on PGP licensing, distribution, copyrights, patents, trademarks, liability limitations, and export controls, see the "Legal Issues" section in the "PGP User's Guide, Volume II: Special Topics".

Contents =====

Quick Overview Why Do You Need PGP? How it Works Installing PGP How to Use PGP

- To See a Usage Summary
- Encrypting a Message
- Encrypting a Message to Multiple Recipients
- Signing a Message
- Signing and then Encrypting
- Using Just Conventional Encryption
- Decrypting and Checking Signatures
- Managing Keys
 - RSA Key Generation
 - Adding a Key to Your Key Ring
 - Removing a Key or User ID from Your Key Ring
 - Extracting (copying) a Key from Your Key Ring
 - Viewing the Contents of Your Key Ring
 - How to Protect Public Keys from Tampering
 - How Does PGP Keep Track of Which Keys are Valid?
 - How to Protect Secret Keys from Disclosure
 - Revoking a Public Key
 - What If You Lose Your Secret Key? Advanced Topics
- Sending Ciphertext Through E-mail Channels: Radix-64 Format
- Environmental Variable for Path Name
- Setting Configuration Parameters: CONFIG.TXT Vulnerabilities Beware of Snake Oil PGP Quick Reference Legal Issues Acknowledgments About the Author

Quick Overview =====

Pretty Good(tm) Privacy (PGP), from Phil's Pretty Good Software, is a high security cryptographic software application for MSDOS, Unix, VAX/VMS, and other computers. PGP allows people to exchange files or messages with privacy, authentication, and convenience. Privacy means that only those intended to receive a message can read it. Authentication means that messages that appear to be from a particular person can only have originated from that person. Convenience means that privacy and authentication are provided without the hassles of managing keys associated with conventional cryptographic software. No secure channels are needed to exchange keys between users, which makes PGP much easier to use. This is because PGP is based on a powerful new technology called "public key" cryptography.

PGP combines the convenience of the Rivest-Shamir-Adleman (RSA) public key cryptosystem with the speed of conventional cryptography, message digests for digital signatures, data compression before encryption, good ergonomic design, and sophisticated key management. And PGP performs the public-key functions faster than most other software implementations. PGP is public key cryptography for the masses.

PGP does not provide any built-in modem communications capability. You must use a separate software product for that.

This document, "Volume I: Essential Topics", only explains the essential concepts for using PGP, and should be read by all PGP users. "Volume II: Special Topics" covers the advanced features of PGP and other special topics, and may be read by more serious PGP users. Neither volume explains the underlying technology details of cryptographic algorithms and data structures.

Why Do You Need PGP? =====

It's personal. It's private. And it's no one's business but yours. You may be planning a political campaign, discussing your taxes, or having an illicit affair. Or you may be doing something that you feel shouldn't be illegal, but is. Whatever it is, you don't want your private electronic mail (E-mail) or confidential documents read by anyone else. There's nothing wrong with asserting your privacy. Privacy is as apple-pie as the Constitution.

Perhaps you think your E-mail is legitimate enough that encryption is unwarranted. If you really are a law-abiding citizen with nothing to hide, then why don't you always send your paper mail on postcards? Why not submit to drug testing on demand? Why require a warrant for police searches of your house? Are you trying to hide something? You must be a subversive or a drug dealer if you hide your mail inside envelopes. Or maybe a paranoid nut. Do law-abiding citizens have any need to encrypt their E-mail?

What if everyone believed that law-abiding citizens should use postcards for their mail? If some brave soul tried to assert his privacy by using an envelope for his mail, it would draw suspicion. Perhaps the authorities would open his mail to see what he's hiding. Fortunately, we don't live in that kind of world, because everyone protects most of their mail with envelopes. So no one draws suspicion by asserting their privacy with an envelope. There's safety in numbers. Analogously, it would be nice if everyone routinely used encryption for all their E-mail, innocent or not, so that no one drew suspicion by asserting their E-mail privacy with encryption. Think of it as a form of solidarity.

Today, if the Government wants to violate the privacy of ordinary citizens, it has to expend a certain amount of expense and labor to intercept and steam open and read paper mail, and listen to and possibly transcribe spoken telephone conversation. This kind of labor-intensive monitoring is not practical on a large scale. This is only done in important cases when it seems worthwhile.

More and more of our private communications are being routed through electronic channels. Electronic mail will gradually replace conventional paper mail. E-mail messages are just too easy to intercept and scan for interesting keywords. This can be done easily, routinely, automatically, and undetectably on a grand scale. International cablegrams are already scanned this way on a large scale by the NSA.

We are moving toward a future when the nation will be crisscrossed with high capacity fiber optic data networks linking together all our increasingly ubiquitous personal computers. E-mail will be the norm for everyone, not the novelty it is today. Perhaps the Government will protect our E-mail with Government-designed encryption protocols. Probably most people will trust that. But perhaps some people will prefer their own protective measures.

Senate Bill 266, a 1991 omnibus anti-crime bill, had an unsettling measure buried in it. If this non binding resolution had become real law, it would have forced manufacturers of secure communications equipment to insert special "trap doors" in their products, so that the Government can read anyone's encrypted messages. It reads: "It is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall insure that communications systems permit the Government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law." This measure was defeated after rigorous protest from civil libertarians and industry groups. But the Government has since introduced other disturbing legislation to work toward similar objectives.

If privacy is outlawed, only outlaws will have privacy. Intelligence agencies have access to good cryptographic technology. So do the big arms and drug traffickers. So do defense contractors, oil companies, and other corporate giants. But ordinary people and grassroots political organizations mostly have not had access to affordable "military grade" public-key cryptographic technology. Until now.

PGP empowers people to take their privacy into their own hands. There's a growing social need for it. That's why I wrote it.

How it Works =====

It would help if you were already familiar with the concept of cryptography in general and public key cryptography in particular. Nonetheless, here are a few introductory remarks about public key cryptography.

First, some elementary terminology. Suppose I want to send you a message, but I don't want anyone but you to be able to read it. I can "encrypt", or "encipher" the message, which means I scramble it up in a hopelessly complicated way, rendering it unreadable to anyone except you, the intended recipient of the message. I supply a cryptographic "key" to encrypt the message, and you have to use the same key to decipher or "decrypt" it. At least that's how it works in conventional "single-key" cryptosystems.

In conventional cryptosystems, such as the US Federal Data Encryption Standard (DES), a single key is used for both encryption and decryption. This means that a key must be initially transmitted via secure channels so that both parties can know it before encrypted messages can be sent over insecure channels. This may be inconvenient. If you have a secure channel for exchanging keys, then why do you need cryptography in the first place?

In public key cryptosystems, everyone has two related complementary keys, a publicly revealed key and a secret key. Each key unlocks the code that the other key makes. Knowing the public key does not help you deduce the corresponding secret key. The public key can be published and widely disseminated across a communications network. This protocol provides privacy without the need for the same kind of secure channels that a conventional cryptosystem requires.

Anyone can use a recipient's public key to encrypt a message to that person, and that recipient uses her own corresponding secret key to decrypt that message. No one but the recipient can decrypt it, because no one else has access to that secret key. Not even the person who encrypted the message can decrypt it.

Message authentication is also provided. The sender's own secret key can be used to encrypt a message, thereby "signing" it. This creates a digital signature of a message, which the recipient (or anyone else) can check by using the sender's public key to decrypt it. This proves that the sender was the true originator of the message, and that the message has not been subsequently altered by anyone else, because the sender alone possesses the secret key that made that signature. Forgery of a signed message is infeasible, and the sender cannot later disavow his signature.

These two processes can be combined to provide both privacy and authentication by first signing a message with your own secret key, then encrypting the signed message with the recipient's public key. The recipient reverses these steps by first decrypting the message with her own secret key, then checking the enclosed signature with your public key. These steps are done automatically by the recipient's software.

Because the public key encryption algorithm is much slower than conventional single-key encryption, encryption is better accomplished by using a high-quality fast conventional single-key encryption algorithm to encipher the message. This original unenciphered message is called "plaintext". In a process invisible to the user, a temporary random key, created just for this one "session", is used to conventionally encipher the plaintext file. Then the recipient's public key is used to encipher this temporary random conventional key. This public-key-enciphered conventional "session" key is sent along with the enciphered text (called "ciphertext") to the recipient. The recipient uses her own secret key to recover this temporary session key, and then uses that key to run the fast conventional single-key algorithm to decipher the large ciphertext message.

Public keys are kept in individual "key certificates" that include the key owner's user ID (which is that person's name), a timestamp of when the key pair was generated, and the actual key material. Public key certificates contain the public key material, while secret key certificates contain the secret key material. Each secret key is also encrypted with its own password, in case it gets stolen. A key file, or "key ring" contains one or more of these key certificates. Public key rings contain public key certificates, and secret key rings contain secret key certificates.

The keys are also internally referenced by a "key ID", which is an "abbreviation" of the public key (the least significant 64 bits of the large public key). When this key ID is displayed, only the lower 24 bits are shown for further brevity. While many keys may share the same user ID, for all practical purposes no two keys share the same key ID.

PGP uses "message digests" to form signatures. A message digest is a 128-bit cryptographically strong one-way hash function of the message. It is somewhat analogous to a "checksum" or CRC error checking code, in that it compactly "represents" the message and is used to detect changes in the message. Unlike a CRC, however, it is computationally infeasible for an attacker to devise a substitute message that would produce an identical message digest. The message digest gets encrypted by the secret key to form a signature.

Documents are signed by prefixing them with signature certificates, which contain the key ID of the key that was used to sign it, a secret-key-signed message digest of the document, and a timestamp of when the signature was made. The key ID is used by the receiver to look up the sender's public key to check the signature. The receiver's software automatically looks up the sender's public key and user ID in the receiver's public key ring.

Encrypted files are prefixed by the key ID of the public key used to encrypt them. The receiver uses this key ID message prefix to look up the secret key

needed to decrypt the message. The receiver's software automatically looks up the necessary secret decryption key in the receiver's secret key ring.

These two types of key rings are the principal method of storing and managing public and secret keys. Rather than keep individual keys in separate key files, they are collected in key rings to facilitate the automatic lookup of keys either by key ID or by user ID. Each user keeps his own pair of key rings. An individual public key is temporarily kept in a separate file long enough to send to your friend who will then add it to her key ring.