"Government Wiretapping, Encryption and the Clipper Chip Debate"

Dorothy Denning, Department of Computer Science, Georgetown University
Robert Holleyman, Business Software Alliance
Michael Gilmore, Supervisory Special Agent, FBI
Ronald Rivest, Department of Electrical Engineering and Computer Science, M.I.T.
Moderator: Stephen Kent, Chief Scientist for Security Technology, Bolt, Beranek and Newman

29 September 1994
Bartos Theatre
Massachusetts Institute of Technology

The following is an edited summary, not a complete transcript of the remarks made by the panelists.

Dorothy Denning (DD): I want to outline the goals of crytography and talk about how well the Clipper Chip would meet those goals. The first goal is strong security or information protection. I was a member of the outside review panel that looked at the Clipper Chip algorithm. Our assessment was that the algorithm looked extremely strong. We couldn't find any weaknesses. However, one of the concerns people have is whether the key escrow system is an area of weakness. In my assessment, enough safeguards are going into the key escrow system that the possibility of a compromise or disclosure of a key will be extremely remote. One of the safeguards, known as "two-person control," plays a role at several stages of the process. This means there would be a high level of assurance that the keys would not be misused. There is also an extensive audit process.

A second goal is that cryptography be affordable. The Clipper Chip is estimated to cost under $10 in large quantities. The cost is higher for the Capstone Chip which is used in the PC MCIA card that is now called Fortezza. However, the cost is not prohibitive for certain types of applications.

A third criteria is that an encryption system should be user-friendly and ready at hand. Right now Clipper Chips are in AT&T phone devices, which involves just pushing a button and the conversation goes into encrypted mode. Using the Capstone Chip with the Fortezza card would be different and would depend on how well it is integrated into the application.

The fourth goal is that it be safe for organizations and individuals. Organizations are concerned about being able to recover their own data and protect against lost keys. Some form of key escrow is therefore necessary, although it does not have to be the government who holds the keys. Right now Clipper just provides for government access to the keys. Individuals cannot go to the escrow agents when they have lost their keys, so Clipper by itself does not meet that objective. But that does not rule out using it with a private sector key escrow system.

A fifth objective is that encryption be safe for society. Wiretaps have been a very useful technique for law enforcement and it would be a mistake for us as a society to lose that capability. The sixth objective is that encryption meet national security goals. Communications intelligence throughout history has served a useful purpose for national security, for example in World War II with the cracking of Germany's codes. In terms of Clipper meeting that goal, since NSA developed it, endorsed it, and put it out there, we can assume that of all the various options that were available this one came the closest.

The final goal is marketability. With the Clipper Chip there is a government market, but the question arises whether the private sector will want it. Some people object that it uses a classified algorithm, it is not open to public scrutiny, or that the government holds the keys. There is also concern that other countries would not be interested in the Clipper Chip.

Many efforts are underway to investigate other approaches to key escrow cryptography. The government has established an industry-government working group to look at alternative approaches to key escrow, and an international key escrow group started meeting this summer. New approaches based on software and on unclassified algorithms have been proposed. Some look promising. Several approaches provide commercial or corporate key escrow services that could meet the needs of corporations.

Robert Holleyman (RH): I want to address two things: 1) the market factors involved in data security, and 2) some of the public policy arguments that have been occurring regarding the current export controls on software with encryption capabilities. I represent leading publishers of software for personal computers including Lotus Development, Microsoft, Novell, and Apple. It is important to recognize how short the evolution of the PC software industry has been. Companies like Lotus went from a small company to a worldwide provider of software and communications products just in the past decade. Encryption capabilities and data security are essential to the functioning of products such as the current flagship product of Lotus, Lotus Notes, and other products that will be marketed in the future.

Unfortunately, we are faced today with an untenable situation in the marketplace. Lotus Notes and other products employing strong encryption algorithms can be sold readily in the United States, but if Lotus or other companies want to market their products out of the United States, they are treated as falling within a munitions category subject to regulation. They are restricted in their ability to sell programs abroad because they can ship a maximum of a 40-bit product, absent a special license. In the United States, DEZ or RC2, RC4 56-bit is roughly the standard that is being used. But foreign purchasers of software are no less sophisticated and no less careful of their privacy than American purchasers.

Thus we can sell strong encryption products in this country but many companies must market a crypto-lite version of any product they sell abroad. The PC software industry has grown enormously in the past decade. Package software companies from the United States have 74 % of the world market for PC software, but that is because they have innovative products which meet the consumer demand. But if US companies cannot market abroad products that meet the demands of consumers in the 1990's and in the century ahead, we will lose those foreign markets as quickly as we have gained them in the past decade.

What we have been seeking is 1) an effort by the Clinton Administration to lift the current export controls that limit the ability of US companies to sell products abroad, and 2) legislation that would force the Clinton Administration to allow the sale of these products abroad. Unfortunately what the Clinton Administration bought into was Clipper Chip and the idea of extending it to data and to products sold abroad. But Clipper has been widely decried by those who have studied it, by the marketplace, and it is not an alternative at the present time to the current export restrictions. We have worked closely with Congress to liberalize the export controls and fight against a possible mandated extension of Clipper to data. In a recent letter to a member of Congress, Vice President Al Gore 1) clarified that Clipper was an approved standard for telephone communications but not for computer and video networks, 2) pledged that the Department of Commerce and the National Economic Council would be involved in studies of the economic impact on the software industry, 3) promised to conduct a renewed effort by the federal government and the private sector to develop a more versatile, less expensive key escrow system that would not rely on a classified algorithm, would be voluntary and would be exportable.

With this set of assurances we feel there is a basis to work together with the Administration to find an alternative to the extension and expansion of Clipper to include data. But each day that goes by, the U.S. loses foreign markets. Surveys shows that as many as 200 foreign producers make hardware or software solutions employing a strong encryption

algorithms. Nearly half of those employ DEZ, and US companies cannot compete in foreign markets against that.

Michael Gilmore (MG): I want to present the view of law enforcement. For us in law enforcement, the issue comes down to access. The Fourth Amendment gives people the right to be secure in their persons, houses, papers and effects from unreasonable searches and seizures. The key concept is the notion of reasonableness. I want to focus on the Title III statute, enacted in 1968, as part of the Omnibus Crime Control and Safe Streets Act, and amended in 1986 to include electronic communications. The statute was passed to protect privacy and to prevent unlawful wiretapping. It also allowed for electronic surveillance to be conducted under very stringent guidelines. The requirements that law enforcement must meet to put in place a wiretap include showing of probable cause, and showing that other investigative techniques have been exhausted or are too dangerous to be conducted. Wiretapping is therefore a last resort type of technique. It is approved by designated senior officials within the Department of Justice and other officials, in my case officials from FBI headquarters, then presented to a U.S. District Court judge for approval. Each application includes the identification of the law enforcement officer, statement of probable cause, the offense and the intended subjects, the communications sought, the nature and location of the communications facilities, an explanation of why the other techniques are too dangerous or ineffective, and the time period.

Once approval is granted, there are very specific procedures governing how law enforcement puts the wiretap in place. One of the requirements is that law enforcement do "minimization". This means that any communication not pertinent to evidence of the crime being investigated is not recorded or listened to. The monitoring equipment is designed to preclude listening while not recording, which would be a violation of the law. Assistance of the service provider is another requirement of the original Title III statute, but with the advances in telecommunications and technology, this requirement is not being met and will not be met if developments continue as they have been. What we are seeking is to maintain our ability to get this assistance set forth in Title III, not to expand our authority.

In 1993, the total number of local, state and federal applications for wiretap orders was about 900. Title III specifies the cases for which authorization will be granted: violent crime, serious criminal activity, terrorist activity, and drug trafficking are the some of the types of cases that will be approved for wiretapping. Although the number of wiretaps conducted is very small, it is a very important technique. Without wiretapping capabilities for those crimes, many of the individuals conducting those crimes would not be brought to justice.

Encryption and digital telephony are access issues for law enforcement. The Clipper initiative applies to the voice communications of the telephone. The only key escrow device currently out there now is the AT&T device, and again it is a voice application. If we gain access to the communication through the technology and assistance of the service providers but we can't understand what is on there, the wiretap becomes useless. An informal study done by the FBI in spring 1994 showed that over the past few years, there were 183 instances where Title III investigations were hampered because of current technology. Whether you call it digital telephony or encryption, it is a public safety issue, and the question is do we want that public safety. I believe we do. As an example, in the past 10 years, 22,000 dangerous felons have been convicted as a result of wiretapping under Title III.

The Clipper Chip is one (encryption) technique that is out there. We have begun discussions with businesses to find out what other options are available for key escrowing techniques. Key escrow appears to be a technique that provides the balance between the privacy of the individual and the need of law enforcement to conduct electronic surveillance.

Ronald Rivest (RR): I want to stay away from specifics about Clipper Chip and talk at a high level about what has been going on over the past 20 years. The government in many ways is systematically attempting to deny Americans the ability to have conversations or records that government can't access. Access is the critical question. If we look at many of the things that have happened — the adoption of the digital signature standard that had no key management

capability, the adoption of the DES — we're talking about the ability of private citizens to communicate or keep records in a way that the government can't access. We're being asked now to trust the government with our most intimate communications. I want to stress that there has been a qualitative change in what's happening. Everything is becoming electronic. When we're talking about preserving the status quo, one has to take into cognizance that everything has been digitized and stored and is available for access.

One of my particular bugaboos is this voluntary bit. Isn't Clipper voluntary? I think a voluntary system is essentially useless for law enforcement or national security because domestic and foreign criminals aren't going to use something that has a key escrow system in it. The proponents of this system are saying it's voluntary; either they are insincere about wanting it to be voluntary, or they are unrealistic about its benefits. I suspect many of the people pushing this program are insincere about wanting it to be voluntary; they want to see it mandatory. However, given the choice of whether to use this or not, I think industry will definitely go elsewhere. We have been seeing that in the market.

Will not the Clipper Chip help the FBI do its job? Maybe. However, I find it rather shocking that the FBI has just asked for a five-year delay to respond to a Freedom of Information Act (FOIA) request regarding its justification for the wiretap bill. It has a number of FOIA requests before it asking for its justification for these things, and it has not responded within the time period that is required by law. So the FBI has been breaking the law with regard to the FOIA requests. Many of the people at the FBI have good intentions. And I support their good intentions. But hell is paved with good intentions and I think one needs to try to figure out what the long-term global impact of some of these proposals is rather than just the near-term battles with some of the particular bad guys that are around. Not everything that helps law enforcement is good for the country.

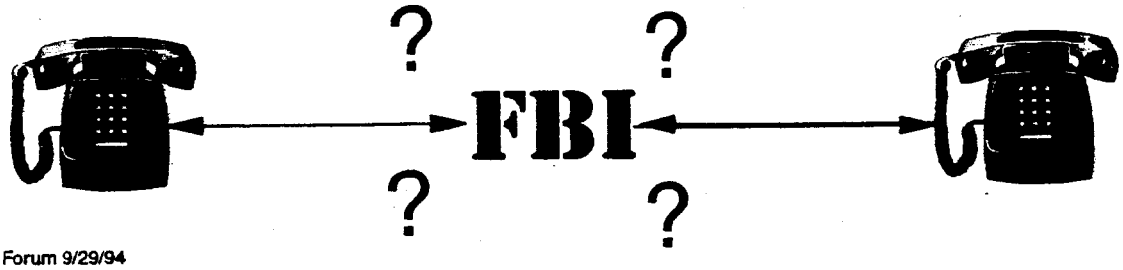
Do I not trust the government? I think it's a traditional American principle to trust the government as little as necessary. Recall there have been many abuses. Recently the IRS has disciplined hundreds of people for abusing the privacy of people regarding their tax returns. Also remember President Nixon. The old statement that power corrupts is the concern here.

I would like to offer what I think is the fundamental question: Should American citizens have the right to have communications and records that the government cannot access even when properly authorized? If you don't believe that people have the right to have truly private records and things, then we can go on the path of Clipper and complete tappability of everything. But if you believe people have a right to some privacy even in the presence of properly authorized government requests, then we can proceed with cryptography as it is proceeding now in the private sector and put aside things like Clipper. To conclude, in view of the ongoing changes in the information infrastructure where everything is becoming digital and subject to access, the Clipper wiretap proposals represent a qualitative change between government and the people, in part because of the amount of information that is becoming available and in part because it is starting to shift the balance of the answer to this fundamental question. I think that poses an unacceptable risk of abuse and these proposals should be rejected.

Beth Rosenson, Student Rapporteur

The Clipper/Wiretap Debate

Ronald L. Rivest
MIT Lab for Computer Science



MIT Communications Forum 9/29/94

Outline

- What's going on?
- Isn't Clipper voluntary?
- Won't it help the FBI do its job?
- What's the deal?
- Don't you trust the government?
- The Fundamental Question
- Conclusions

What is going on?

- The government (NSA, FBI, etc.) is attempting to systematically deny Americans the ability to have conversations or records that the government can't access.
- We are asked to trust the government with all of our most intimate communications.

Isn't Clipper voluntary?

- A voluntary system is useless for
  - law enforcement
  - national security
- Proponents are either insincere about wanting it voluntary, or unrealistic about its benefits.
- Given choice, industry will go elsewhere.

Won't it help the FBI do its job?

- The FBI has just asked for a five-year delay to respond to a FOIA request regarding justification for the Wiretap Bill.
- The FBI has not responded to FOIA requests in these matters in accordance with the law.
- Hell is paved with good intentions.
- Not everything that helps law enforcement is good for the country.

What's the deal?

- You get
  - Some (?) assistance to law enforcement and national security
- by
  - giving the government the keys to all your most intimate conversations and records.

Don't you trust the government?

- As little as necessary!
- Recall:
  - CIA/Aldrich Ames
  - IRS/scandal
  - President Nixon/Watergate
  - FBI/Martin Luther King
- Power corrupts.

MIT Communications Forum 9/29/94

The Fundamental Question

- Should American citizens have the right and ability to have communications and records that the government can not access (even when "properly authorized")?

☐ **YES** ☐ **NO**

The Fundamental Question

- Should American citizens have the right and ability to have communications and records that the government can not access (even when "properly authorized")?

Denning	☐ YES	☐ NO
Holleyman	☐ YES	☐ NO
Kallstrom	☐ YES	☐ NO
Rivest	☑ YES	☐ NO

Conclusions

- In view of the ongoing changes in our information infrastructure, the Clipper/Wiretap proposals represent
  - a qualitative change in the relationship between the government and the people, and
  - an unacceptable risk of abuse.
- These proposals should be **REJECTED.**

Recommended Readings

- *Information Security and Privacy in Network Environments* (Office of Technology Assessment, 9/94)
- *Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy* (ACM U.S. Public Policy Committee, 6/94)