UNIVERSITY OF WISCONSIN MILWAUKEE

College of Engineering and Applied Science
Dept of Electrical Engineering and Computer Science

September 24, 1993

Director, Computer Systems Laboratory
ATTN: Proposed FIPS for Escrowed Encryption Standard
Technology Building, Room B-154
National Institute of Standards and Technology
Gaithersburg, MD 20899

Dear Mr. Director:

I want to take this opportunity to express my concerns about and opposition to the "key escrow" proposal that enables the government to eavesdrop on the communications of Americans with the Clipper encryption technology.

The proposed bugging of data and voice communications of the nation is being presented as a necessary measure to supposedly protect "law enforcement" and "national security" interests.

What is being proposed threatens one of the most fundamental constitutional rights: the right to privacy. There is a tendency to view cryptography as a weapon, the official view of the intelligence agencies. That is no more true for cryptography than for ordinary locks and keys, since, after all, cryptography pertains to the design of locks and keys for data protection. The fact of the matter is that many of our assets are no longer physical, but *logical.* If we allow the constitutional protection against search and seizure to lapse just because technology has changed the nature of certain things would mean that we have to throw away a great many parts of the constitution because new technologies can change other concepts of where one's possessions and even physical self begin and end.

There is widespread agreement that criminals, especially smart ones, will not use a bugged device to conduct their business. It is important to consider the options of the criminal. Does the criminal have to use the bugged system? The answer is certainly no. Criminals, especially the ones that are being touted as the targets of the system, drug dealers and terrorists, are well funded. They will have no problem getting com-

PO Box 784 • Milwaukee, WI 53201

CS Tel: 414 229-4677
EE Tel: 414 229-5252
FAX: 414 229-2960

puter hackers to build them hardware and software systems to implement their own cryptographic systems. Computer specialists are hardly more immune to the lure of money or intimidation than other professionals. Moreover, if cryptography is essentially outlawed, as is being contemplated in FOIA obtained internal memoranda of the government, then the only people with access to quality cryptographic systems and services will be criminals. To paraphrase that old battle cry, "If you outlaw cryptography, only outlaws will have cryptography". Not only can criminals encrypt their messages, they can also hide the ciphertext with techniques of information theory to make it look innocuous. Already the effects of government control is taking its toll on research in cryptography: the number of papers on design of new systems is miniscule compared to the number of papers that deal with the one or two systems in place. In addition, the availability of hardware and software, that is sorely needed for the protection of computer systems and data, is so limited given our incredible technological advances that from a protection point of view we are in fact a "cryptographic third world".

In view of the fact that criminals will have access to the technology that is being denied law abiding citizens, one must ask then: just what targets will be left to evesdrop on? Ordinary Americans, politicians, dissidents, labor leaders, ...to name a few. This proposal, when considered with its monster twin, the proposed digital signature standard, DSS, a sort of government approved no-other-pens-allowed BIC pen, amounts to a national dragnet.

Some supporters of this major violation of privacy say that it is no worse than, say, arrest. It is absolutely worse than arrest. It is done secretly. It attempts to predict that a person is about to commit a crime. If the right to privacy can be violated on suspicion that a crime might be committed, other rights will be violated too. It is difficult to see how one can draw the line at just privacy, one of the most sacred rights in this country. There is no doubt as to what is next: preventive detention; observe how people walk, talk and think to themselves and put them away, well before they have done anything.

The consequences of privacy violations is not all that apparent to some members of the crypto community. Some may be unaware of the bugging, ridicule and assault of even prominent members of the various minorities. One hardly needs to mention the bugging of Martin Luther King, harassed by the FBI. But some might say that was in the past. Well one does not have to go back that far in time. More recent events involving a Governor of a State show that this type of intimidation is continuing. As the country's multicultural pot becomes ever more mixed, we hardly need to put in place tools for abuse of one race or religion by another that may be momentarily in control of the devices.

Still other Americans have been the subject of bugging, allegedly by foreign governments. Consider the case of Andrew Young, the US ambassador to the United Nations. He was forced to resign, allegedly because his conversations were bugged by Israel. If someone of the rank of ambassador can be brought down, it is difficult to imagine how anyone can be safe. Other governments will no doubt have a stake in getting rid of government officials who don't suit them. Dissidents from other countries who take refuge here will hardly be safe with such a wholesale bugging system. After all intelligence agencies cooperate with even the most human rights abusive governments. Such governments will no doubt need "favors" from time to time.

It is interesting to note that at the CRYPTO-93 meeting, fear was expressed that the "Biden" bill might become reality. This was in reference to an attempt by Senator Joseph Biden to put severe restrictions on the use of cryptography. Senator Biden is chairman of the Senate Judiciary Committee, which blocked the nomination of Judge Robert Bork to the Supreme Court because of concern about *privacy*. This is certainly a change in perception of just who is a threat to privacy.

Finally, even the very name of this proposal for systematic bugging, "escrow", is deceptive. Consider the very definition of "escrow" (Webster's dictionary):

- a deed, a bond, money, or piece of property held in trust ...

Privacy held in trust? By Police? By Intelligence agents and their friends? It is impossible to imagine how one's privacy can be taken back after it is violated. Holding privacy in escrow is like holding someone's wife in escrow for a night. This is no escrow. This is an indecent proposal.

Sincerely

George I. Davida
Professor

cc: