Personal privacy may be permanently eroded by the Clipper chip.

New Initiatives which May Erode Your Privacy:

Or George Orwell Was Off by Only a Decade

Kenneth P. Weiss

Information Management & Computer Security, Vol. 2 No. 3, 1994, pp. 43-45
© MCB University Press Limited, 0968-5227

Expensive, flawed technology is being aggressively proposed by the US administration which may permanently erode personal privacy and will not accomplish its stated goal. It is generically referred to as the Clipper chip.

The Clipper chip is a microchip technology developed by the US National Security Agency (NSA) which is intended to be embedded in most communication devices. Clipper will provide some level of automatic encryption (privacy protection) for the average user. However, each chip will have its secret decryption key escrowed with government agencies which will allow the possessor of the key to clandestinely observe or listen to the unencrypted private information. Presumably there is only one key, with no "back door" method for surreptitious access, and the keys would be available to law enforcement only through the equivalent of a court order. It is proposed that, in the future, these chips be integrated into virtually every form of communication equipment: telephones, cellular and radio telephones, video equipment, facsimile machines, computers and computer networks and information storage equipment.

There is now a major controversy between some government agencies who are involved in an aggressive campaign to force new encryption standard and influence legislation for imposing the technology, and the chip's adversaries. These adversaries include independent scientists, academicians, manufacturers of computer and communications equipment, privacy groups, civil rights groups, many members of Congress and professional organizations and diverse informed individuals. All, almost unanimously, criticize or condemn the Clipper technology and the campaign to foist it on American society.

Some law enforcement professionals and those charged with protecting our national security argue that they have never had greater challenges in implementing their responsibilities in the "information age". The Constitution gives the Government the right, in certain circumstances, to limit the rights, privacy and freedom of its citizens for the greater social benefit. Unfortunately, Clipper technology will not have the desired effect for law enforcement but will set a dangerous precedent and permanently erode privacy in our society.

The geometric growth and implementation of computer and low-cost encryption technology in the information age and the emerging information superhighway have clearly made it more difficult for law enforcement to "eavesdrop" in certain circumstances. Increased difficulty for law enforcement is not justification for eroding or jeopardizing rights derived from the Fourth Amendment.

Without speculating on or impugning the motivation and integrity of the current advocates of the Clipper chip, it is obvious that neither they nor we can guarantee the motivation or integrity of future custodians of this technology. This is particularly true, given the historical examples of abuse and the inevitability of temptation. *Quis custodiet custodies*?

The ever-increasing communications bandwidth heralds the fact that every aspect of our personal, professional, social and leisure activities will be inextricably integrated in the information age. With Clipper this information will be vulnerable to abuse and exploitation. The Clipper chip is a very bad idea!

Seven Reasons Why the Clipper Chip is a Bad Idea

(1) *The concept.* The concept is incompatible with the privacy and freedom from inappropriate government scrutiny that Americans have a right to expect. There is little qualitative difference

between the Clipper proposal and one which would mandate that the keys to your home, office, filing cabinet, diary and the combination to your safe be escrowed with government agencies, to be available to law enforcement for clandestine use – with permission from a judge. Whatever difference is perceived to exist is associated with assuming a false distinction between privacy of person or private tangible property and private information or private communication.

(2) *Business considerations.* The Clipper chip (a) will increase product cost, design complexity and require additional power and space considerations at a time when computer and communications devices are becoming smaller and power is at a premium, and (b) will further affect and erode the ability of US manufacturers to compete in the global marketplace. What foreign company or government would purchase a US product knowing that the US Government held the keys to its security?

An additional business consideration, of crucial importance, is the fact that the arena available to Clipper's eavesdropping is going through geometric expansion. As broadband fibreoptic links are bought into use, a much larger percentage of the internal activities of American business will be transmitted between and among dispersed units of corporate enterprises and between co-operating groups of independent professionals such as physicians, lawyers and the news media.

With Clipper, the government has the potential to insert itself right in the middle of this internal group discussion and business traffic (as opposed to external communication) but without the sort of specific area-by-area authorization that such intrusive oversight would require today. After the universal implementation envisioned for Clipper, without additional layers of privacy technology there will be little refuge.

(3) *Slippery slope.* If ever a policy and technology carried with it the likelihood that it was the beginning of a series of policies which were likely to erode our fundamental privacy and freedom – the Clipper chip is it. It's archetypical! The government is attempting to create a *fait accompli* by shrewd implementation of the technology, *before* congressional action, in certain sectors under its influence or control. This ploy highlights the potential and motivation for further extending such inappropriate policies and technologies into new arenas in the future.

(4) *Abuse and misuse.* The government track record of misuse and abuse of its power and authority is well established and each day new revelations suggest that the problem is now both endemic and far worse than ever expected. Of particular concern is the existing initiative to provide direct communication channels into FBI headquarters. This will allow the simultaneous rerouteing of any number of private communications, from anywhere in the country, to be monitored or put under surveillance easily, and at any time.

Assuming that a court order is necessary to obtain keys, there is nothing to prevent recording and storing information and conversations at from *any* time in the past, then obtaining the keys for some current reason and playing back all previously recorded conversations. How do you preclude future eavesdropping, by sophisticated individuals, once keys are made available for a legal limited specific purpose? Imagine if the FBI under Hoover had the Clipper chip to abuse and use for extortion. *"Those who cannot remember the past are condemned to repeat it".*

(5) *The wall of secrecy.* The wall of secrecy that NSA has created around the algorithm by not exposing it to traditional academic and professional scrutiny is such that no one can assume the strength or robustness of the algorithm or preclude the possibility of a back door. Indeed, flaws in the technology, which defeat the intended purpose, have already been detected and published by one scientist. Another group has reverse-engineered the supposedly non reverse-engineerable chip.

Furthermore, even if we assume the integrity, positive motivation and critical cryptographic expertise of the few outside evaluators selected by NSA to review the code and speak publicly on its behalf, the continuing secrecy surrounding the code actually inside the chip does not preclude the possibility of clandestine substitution of the evaluated code for one with a back door during actual chip production. Indeed, one might reasonably argue that NSA's legal charter for "national security" mandates that they seize the opportunity to clandestinely subvert such a technology.

(6) *Challenges.* The argument that law enforcement needs the Clipper technology to effectively meet modern challenges has little merit. Requiring an expenditure of some effort, time and resources before pre-empting rights of privacy is part of the legitimate burden of a free society. Challenge for law enforcement and government agencies has always created economic opportunity, stimulated technological advances, innovation and new spin-off products which ultimately benefit society.

(7) *Clipper's relative effectiveness.* Criminals and subversive elements targeted by this technology

> will not be affected under the Clipper chip proposal. Use of the existing, off-the-shelf, low-cost encryption products (supplemental to communications equipment with the Clipper chip embedded) severely limits government eavesdropping. This fact alone ensures that the Clipper chip is, indeed, a slippery slope technology.

It follows that in the future the Government has to be poised first to require Clipper by law and next to outlaw all other forms of privacy protection and encryption; otherwise the enormous investment proposed here will be unproductive. And of course the most targeted groups – the terrorists, drug lords, espionage agents and other criminals – are not about to be stopped by an intrinsically unenforceable law. Just as it is currently technically illegal to export a book of random numbers, a likely consequence of the Clipper proposal is the eventual legal suppression of academic cryptographic information and associated mathematics. An encryption product black market will become a major industry.

Why don't we hear both shoes drop in this proposal? Why propose the Clipper chip first, when anyone really understanding the issues discerns that Clipper alone doesn't do the job? The answer is that outlawing all encryption and privacy products will have serious constitutional and political implications – implications which may become more saleable to Congress and the public after hundreds of millions of taxpayer dollars are already committed to Clipper chip installations.

The Clipper chip should be torpedoed!

Kenneth P. Weiss is the founder, Chairman and Chief Technical Officer of Security Dynamics, Cambridge, MA, USA. He is a member of the editorial boards of the *Journal of Information Systems Security* and *Information Management & Computer Security.*