

**Subject:** USACM Memo Regarding Encryption - please circulate to CIC

October 2, 2001

**To:** Members of the U.S. Congress, Congressional Internet Caucus

**Fr:** U.S. Policy Committee of the Association for Computing Machinery (USACM)

**Contact:** Jeff Grove, Director of Technology Policy, USACM, (202) 659-9711

**Re:** Government Controls on Encryption

The widespread use of strong encryption is fundamental to the protection of our nation's critical infrastructures and should not be impaired by the establishment of a mandatory key-escrow system or imposition of "backdoors" in the algorithms. There are strong technical reasons to believe that any such restrictions are both unworkable and unenforceable; but what is more important is that any attempts to do so will hurt legitimate U.S. security needs and damage the U.S. economy.

Strong encryption is critical to worldwide commerce and interaction. The technology of scrambling data and messages has become a crucial element of computer security for businesses and consumers alike because of demands for private and secure communications. It is embedded in software and hardware, and various forms are standardized. Retroactively altering products to meet key-escrow or recovery requirements would cause significant and costly disruptions to the flow of data, goods, and services throughout the economy, if it could even be implemented in a timely fashion. In addition, such actions may erode consumer confidence in on-line transactions.

Secure cryptographic systems are notoriously difficult to design. Some older systems that were in common use for years were discovered to have hidden weaknesses after prolonged study. The cryptographic algorithms and protocols in current use have taken considerable time and effort to verify and implement. Imposing algorithms with backdoors that are largely untested may introduce unintended weaknesses that will not be discovered immediately. Furthermore, the escrow or recovery mechanisms themselves may actually be compromised by criminals, with unfortunate results.

Any encryption restrictions would be costly to U.S. companies supplying encryption-enabled products to the world. Today, there is a large worldwide demand among law-abiding customers for strong encryption. However, foreign markets have repeatedly indicated that they are unwilling to accept U.S. products limited by key-escrow or "backdoor" schemes, especially as there are companies in more than 20 other nations offering similar products without such "features." U.S. companies would suffer a loss of market as a result.

Last of all, any restrictions will be largely ineffective as criminals and terrorists would still have access to hundreds (if not thousands) of existing encryption products and shareware. In fact, strong cryptographic protocols are so well-known, even relatively

unsophisticated users will be able to re-implement them. Legislation against using strong encryption will have as much effect on terrorists and criminals as do current laws against use of weapons in commission of crimes.

In summary, we observe that most citizens and businesses in the U.S. now depend -- directly or indirectly -- on strong cryptography to protect their safety, security, finances, and privacy. It is not technically feasible nor is it in the best interests of the U.S. Government or people to attempt to impose weaknesses on encryption technology or use.

The ACM is a leading society of computer professionals in education, industry, and government. The USACM Public Policy Committee facilitates communication between computer professionals and policy-makers on issues of concern to the computing community. For more information, please contact the Jeff Grove, Director of the ACM Washington Policy Office at (202) 659-9711 or see the USACM policy web site at: <http://www.acm.org/usacm>