

AMERICAN FOR COMPUTER PRIVACY

STRONG ENCRYPTION IS NEEDED IN ORDER TO SECURE NETWORKS AND PREVENT FUTURE TERRORIST CYBER-ATTACKS

Summary

All of ACP's members -- 100 companies, 40 associations and interest groups, and 7,000 individuals -- deplore the September 11th murderous physical hijacking and suicide crashing of four airplanes. Many of ACP's members have been helping the Government with technical expertise and donations of equipment and money in the aftermath of the September 11th attacks. ACP is concerned that a future attack could be launched from a distant foreign country by means of the Internet on computer networks controlling key aspects of American life.

Encryption is the technology that protects critical computer networks and information against terrorist attacks and criminal hackers. The widespread use of encryption promotes our national security and prevents crime by ensuring the security, confidentiality and authenticity of electronic networks, information and users. The use of American security technology also ensures the availability of American companies and technical experts in times of trouble.

Encryption also is essential to the U.S. economy and millions of jobs. American businesses and consumers have become dependent on computer networks, the Internet and e-commerce. Encryption protects confidential business information and is critical for e-commerce to develop. Encryption also protects the personal privacy of Americans in the electronic age by guarding their sensitive information on-line.

Clearly some terrorists and criminals may use encryption to hide their plans and activities. But proposals to restrict the use of encryption would weaken our ability to defend ourselves and would not keep encryption out of evil hands because there are hundreds of products available around the world and for download off the Internet. Reimposing unilateral U.S. export controls would simply give the encryption market to foreign companies but would not keep encryption from terrorists. Requiring an extra set of encryption keys to be held "in escrow" by a third party would weaken cybersecurity for everyone except the terrorists who would not use it.

The Next Attack Could Be A Cyber-Attack

Technology has made many of our Nation's essential services enormously more robust and reliable. But the same "interconnectedness" that has greatly increased efficiency and productivity has also given rise to increase vulnerability. Today the United States is dependent on private sector information and computer networks, products and services that make up the critical information infrastructure. A future attack won't have to use planes or bombs – it could use keystrokes to target the cyber-systems at the heart of operation and control of our nation's critical infrastructures.

There were reportedly thousands of planes in the air on September 11th – what if suddenly they found themselves with no guidance or remotely controlled. Or a cyber-attack on the computer networks controlling the nation's telecommunications or financial services, the power grid of water distribution system for several states, or the hospitals in a major city.

The private sector developed, owns and operates most of our nation's critical information infrastructure and has the experience and expertise to protect it. American companies continue to be hard at work using technology to secure the net!

Encryption Is An Essential Component of Cyber Security

Encryption is the technology that protects critical computer networks and information against terrorist and criminal hackers. The widespread use of encryption promotes national security and prevents crime by ensuring the security, confidentiality, and authenticity of electronic networks, information and users. Quite simply, without strong encryption it is impossible to adequately secure these networks and information. Equally importantly, the use of American security technology ensures reliance on American companies and technical experts – many of whom have been helping the Government in the wake of the September 11th attacks.

For all these reasons, over the last several years the consensus among policymakers in Washington has been to promote the widespread use of encryption. As early as 1996, a National Research Council "wise men" report called for the "broad use of cryptography" to meet information security needs. "If cryptography can help protect nationally critical information systems and networks against unauthorized penetration (which it can), it also supports the national security of the United States." Similarly, a 1999 study by the Center for Strategic & International Studies led by former FBI and CIA director William Webster concluded that "an extraordinarily important part of the emerging environment will be the widespread use of robust, strong encryption."

A majority of Congress supported the adoption of a new encryption policy which included the ability of American companies to export encryption products. The Administration's decision to adopt such a new policy in 2000 was supported by the defense, intelligence, law enforcement and commerce departments.

Proposals To Limit The Use of Encryption Would Weaken National Security

Some terrorists and criminals are known to use encryption to hide their activities. This leads some to call for limiting the use of encryption. Yet such proposals are both impractical given the availability of encryption around the world and on balance would weaken our national security.

1. Reimposing Unilateral US Export Controls Would Give The Encryption Market To Foreign Companies But Would Not Keep Encryption From Terrorists

Throughout the 1990's the U.S. Government imposed unilateral export controls on American encryption products. The result was to foster the creation of a vibrant foreign encryption industry. By 1999 there already were more than 800 foreign hardware and software products manufactured in 35 foreign countries at least 167 of which used very strong encryption. There were 512 foreign companies manufacturing or distributing foreign cryptographic products in at least 67 countries outside the U.S. These products were as good as the American products. Foreign companies had begun marketing to U.S. customers based on the inability of American companies to sell strong encryption products worldwide. Strong encryption products also were (and are) available for download off the Internet.

Clearly U.S. policy was not keeping strong encryption out of the hands of anyone who wanted it. It simply was keeping strong American encryption products off the market. That's why as early as 1996 a National Research Council "wise men" report warned that U.S. export controls would harm both U.S. national security interests and U.S. businesses and industry. In 1998 the Economic Strategy Institute warned that export controls would cost the U.S. economy \$40- \$97 billion over the next five years.

In 2000 the U.S. government permitted the export of American encryption products to legitimate users in most countries and continued prohibitions on exports to terrorist countries or to suspect persons. This conformed U.S. export control policy to that of the EU (although both remained stricter than other countries).

2. Requiring "Key Escrow" Encryption Would Weaken Cybersecurity For Everyone Except the Terrorists Who Would Not Use It

Some accept the need for strong encryption but also want to ensure easy government access to information in cases of suspected terrorist or criminal communications. They would require an extra decoding key to be kept with a third party where the government could get it when needed. But such so-called "key escrow" proposals all suffer a fatal flaw: they reduce the security of the network. There are numerous security problems associated with managing all the extra keys. These systems also necessarily create rich new targets for cyber-attacks – whoever holds the extra keys!!

A 1998 report by eleven of this country's top cryptographers and computer scientists concluded that key escrow encryption "will result in substantial sacrifices in security and greatly increased costs to the end user. Building the secure computer-communication infrastructures necessary to provide adequate technological underpinnings demanded by [law enforcement] would be enormously complex and is far beyond the experience and current competency of the field. Even if such infrastructures could be built, the risks and costs of such an operating environment may ultimately prove unacceptable. In addition, these infrastructures would generally require extraordinarily levels of human trustworthiness. These difficulties are a function of the basic government access requirements proposed for key recovery encryption systems. They exist regardless of the design of the recovery systems. . ."

Finally, all such proposals also ignore the basic fact that terrorists or criminals will not use a key escrow encryption system when they have available hundreds of encryption products from dozens of foreign suppliers and off the Internet.

Encryption Is Essential to The U.S. Economy

In the last few years American businesses and consumers have become dependent on computer networks, the Internet and e-commerce. Andy Grove's prophesy that every company will be an Internet company has come true whether it's for internal operations, B2B or B2C commerce. Multinational corporations, small businesses and other organizations use computer networks and the Internet to inform employees about medical benefits and company developments, buy and sell materials, bid for services, recruit new business and invoice customers.

But e-commerce simply does not occur without good security. Lack of it was one of the major impediments to the growth of e-commerce. Encryption is a fundamental building block of the digital age and the widespread use of strong encryption is critical to the future of the economy and millions of American jobs. A strong American industry also means keeping cybersecurity expertise and experience right here at home.

An already weak economy is now reeling from the impact of the September 11th attacks. Limiting the use of strong encryption would delay and reduce economic growth.

Encryption Is Essential To Protect Personal Privacy In The Electronic Age

Americans continue to feel strongly about the need to protect their electronic information against unauthorized access and attacks. They use the Internet to pay bills, file tax returns, buy and sell stocks, purchase new cars, order groceries and email their children at college. Social Security numbers, driver's license numbers, bank account information, credit reports, PIN numbers, wills and other legal documents are all stored on computers. Doctors and hospitals store sensitive medical data online and email records to remotely located specialists. Pharmacies file patient prescriptions.

Two polls conducted just days after the September 11th attacks continued to show strong majority support for the privacy of electronic communications. While majorities of Americans in the New York Times/CBS and Pew Research Center polls said they would give up some civil liberties to fight terrorism, 71% and 70% respectively opposed government monitoring of emails and phone conversations.

September 25, 2001