# Security vs privacy in the internet

The question of privacy began when man uttered his first words. The question was raised again when the postal system began and then when telephones were introduced. Once again, we must apply the question to the new information superhighway, that is e-mail, telecommuting, online newsgroups, etc. The question is this: How important is privacy on the Internet According to Webster’s Ninth New Collegiate Dictionary, privacy(1) is “ freedom from unauthorized intrusion. ” It is an issue that always concerns people. Several forces determine privacy.

The two primary forces – cultural principals and governmental regulation – constantly battle with each other to satisfy this longing for “ freedom from unauthorized intrusion. The government collects a considerable amount of personal data on individuals, for example drivers licenses. Similarly motor vehicle registration agencies collect information about a persons name, address, date of birth, Social Security number, physical description and even the make, model, and loan for their automobile. Patient medical information is collected for various Government agencies.

Court records are also a major source of information because criminal matters, divorces and wills often place a wealth of personal details into the public domain. The collected data is stored in large computer databases and can be accessed at click of a mouse button by all the Government officials. The downside, however, is that some corrupt official, for personal hatred, can find out from this database where a particular person lives. He/she might use this information to vandalize that persons private property. The private industry has access to all the public records.

A wealth of information is also collected from consumers visiting commercial web sites. Companies feel personalization empowers them to better understand their customers' needs and desires and improve customer service by tailoring offerings to the unique needs of individuals. Private companies that collect personal data might ensure privacy, but at the same time they may share that information with some other partner company. The second company might not be of individuals interest but he/she might still get junk mail from that company.

According to the 1999 Georgetown Internet Privacy Policy Survey, 93% of the websites collect personal information, 44% of the overall websites post privacy policies and only 10% comply with all fair information practices recommended by the Federal Trade Commission(2). The Government, thus to ensure privacy to an individual, must lay down stricter rules for the private industry. While privacy may be a concern in the private sector it has a higher price when it comes to national security.

Leading security experts predict that it is only several years before a terrorist or rogue nation is capable of an online, hacker-style attack against the United States, causing extensive failure of such crucial elements as banking or the financial markets, transportation systems, the power grid or telecommunications. The Federal government needs to step up measures to protect critical information systems from fraud and misuse, sensitive information from disclosure and critical operations from disruption.

In order to accomplish this government feels the necessity to intrude into peoples personal lives through use of encryption. Encryption is technology

that “ encodes” computer data so only the owner can control who reads them. Access to encrypted files or email requires the use of “ keys,” like your bankcard PIN number provides computerized access to a bank account. The Government’s proposition is to have easy access to everyone’s keys and store them in a large database (typically referred to as key escrow) so that they can decrypt messages when They determine there is a reason to.

Another proposition is to put the keys in the hands of government-approved “ third parties. ” While protective measures are necessary, I do not agree with the above-mentioned government plans. Any bill that Congress passes affecting encryption should ensure that American citizens, businesses and institutions can continue to buy and use the strongest encryption technology available to protect themselves, their customers and their stakeholders from crime, without fear of unwarranted government intrusion.

Computer technology has rapidly become a fundamental element of day-to-day life. Encryption is what protects computer files and communications from eavesdroppers, thieves and other criminals. Following are the reasons why governments encryption plans show not be introduced. if Congress allows government to hold encryption “ keys,” that are subject to a warrant, it would do more than allow court-ordered wiretaps. It would require you to store computer data only in formats that law enforcement can easily understand and conveniently access, often without your knowledge.

It would provide law enforcement greater access to private information, which is fundamentally intrusive and threatens our constitutionally protected right to privacy. No government policy can ensure that encryption “ keys”

deposited with “ third parties” will be handled responsibly. As the number of keys that would require proper storage multiplies daily, reaching into the billions, holding “ third party” key-holders accountable would be virtually impossible.

If strangers could unlock encrypted computer files containing confidential information about you – whether stored at your home, a hospital, an insurance company or bank – that information could fall into the wrong hands. Health records, credit card numbers, credit histories and tax information protected by encryption could all become more vulnerable to misuse. The U. S. Government has various restrictions on the export of most encryption products.

Today, while that policy hamstrings U. S. manufacturers, companies from more than 20 other nations have developed hundreds of products to take advantage of the booming demand among law-abiding customers for strong encryption. These restrictions have cost the U. S. billions of dollars in revenue and hundred thousands of high-skill, high-wage jobs. As the Internet grows throughout the world, more governments may try to impose their views onto the rest of the world through regulations and censorship.

If too many regulations are enacted, then the Internet as a tool will become nearly useless, and our mass communication device, a place of freedom for our mind’s thoughts will fade away. We must regulate ourselves as not to force the government to regulate us. If encryption is allowed to catch on, there will no longer be a need for the government to intervene on the Internet, and the biggest problem may work itself out. As a whole, we all

need to rethink our approach to privacy and allow the Internet to continue to grow and mature.