How can the government protect public safety without access to keys that decode encrypted data?

Surveillance--the clandestine interception of information--is a vital national security tool to protect against terrorism in times of peace and to insure victory in times of war. Virtually all digital information and communication today can be encrypted, making it unreadable to anyone without a key, so that effective surveillance is difficult or impossible

Encrypted information—codes and code breaking—have played a critical role in every war fought by the United States since the Civil War in the 1860s. Electronic eavesdropping has also played a critical role in national security and criminal investigations. Wiretapping was first used during a period of perceived national emergency—the first World War. Since that time, law enforcement has had a long history of reliance on electronic surveillance, particularly to enforce Prohibition and to investigate organized crime. Wiretapping laws include safeguards to protect a citizen's right to privacy and to due process, including restricting wiretapping to certain crimes and requiring a court order based on probable cause. Data is maintained on electronic surveillance beyond the life of the investigation to accommodate the appeals process, Freedom of Information Act requests, etc. Beyond domestic law enforcement, advanced electronic surveillance techniques—so called "espionage tradecraft"-- have been developed to monitor the behavior of foreign espionage agents and hostile countries. This surveillance is largely governed by the Foreign Intelligence Surveillance Act (Title 50 USC5). Advanced surveillance technologies of the time were used to prove the Soviet Union's culpability in shooting down KAL Airlines flight 007 in 1983.

Today, almost any information can be shared digitally. The sharing of digital information is complicated not only by the public nature of its transmission, over a commonly shared international network, but also by the fact that digital information can be easily and undetectably modified. Encryption algorithms are used to convert eye-readable plaintext to a form that cannot be read or modified without decryption, and for conversion back to plaintext once the message is received. Encryption is used to insure confidentiality and to prevent tampering with digital information. Sometimes only a "signature" is encrypted, to authenticate that a document has been sent from a particular person or a message digest is created and attached to a message, to show that the unencrypted message has not been altered.

Keys combined with an algorithm are used to encrypt and decrypt information. Symmetric encryption uses a shared private key—to both encrypt information for sending and to decrypt information upon receipt. Asymmetric encryption uses two keys—a public key and a private key. The private key holder distributes public keys to those with whom (s)he wishes to communicate. The more bits used in the key, the harder it is to locate a particular message key through an exhaustion attack to identify the correct key among all the incorrect possibilities.

A large key can be virtually undiscoverable, given the current speed and processing capabilities of key discovery software programs and computer platforms.

The federal government is in a difficult position with regard to encryption. On the one hand, the federal government is responsible for safeguarding the nation's information assets, many of which directly impact national security and public safety. The federal government has traditionally promoted encryption standards as part of a suite of Federal Information Processing Standards (FIPS). DES, a widely-used encryption standard, was developed by IBM and endorsed by the National Security Agency (NSA) as FIPS 46.

The NSA and the National Institute for Standards and Technology (NIST) share responsibility for encouraging the development and promotion of encryption algorithms as FIPS standards. Currently, NIST and NSA are in the public comment period on proposals from five finalists for an Advanced Encryption Standard (AES), being touted as "a crypto algorithm for the twenty-first century." (1)

At the same time, the virtually unbreakable character of high-bit encryption algorithms can mean a serious compromise to national security, in that hostile governments, terrorist organizations, criminals and spies can encrypt information and communications of any nature, making it impossible for the government to monitor threats to national security and public safety. In addition, current laws governing wiretapping and electronic surveillance must be updated to accommodate encryption technologies. President Clinton and the Justice Department, particularly Attorney General Janet Reno and FBI Director Louis Freeh, have pushed for legislation that would enable electronic surveillance involving encryption. They have promoted the Cyberspace Electronic Security Act (CESA), which would, among other things, protect sensitive investigative techniques and trade secrets from public disclosure in court and greatly enhance the FBI's ability to perform cryptoanalysis to decrypt information through key discovery programs. They note that when privacy and security clash, citizens are frequently willing to forgo privacy for personal safety. An often-cited example are the increased controls at airports, where people must pass through metal detection gates, subject their baggage to X-ray and inspection, show identification and answer questions about their luggage. There have been very few complaints about increased security at airports because citizens believe their safety is being directly impacted by tighter security.

The government has also actively promoted the concept of a key escrow program, which would retain keys to all encryption used in the United States, so that the government could perform anonymous electronic surveillance by decrypting encrypted communications when due cause could be proven. The important concept is that of anonymous surveillance, which is critical for obtaining incriminating or corroborating information. If an encryption key remains

undiscoverable, the government must request a key to decrypt information. This defeats the purpose since the surveillance is no longer anonymous and thus unlikely to be useful.

The government's key escrow program came under immediate attack by civil liberties organizations and U.S. businesses. Among other arguments, these groups pointed out that the federal government has a dismal record of protecting their own networks from intrusion. A key escrow system under government management would present a single point of failure for determined criminals or foreign spies wanting access to a range of encrypted information, from stored credit card and ATM PIN information to confidential research and development in industries and universities. Civil liberties organizations pointed out that the government would have access to information privately encrypted by individuals that was not retrievable by the employers or colleagues of those individuals. Information about encrypted communications would be documented and stored, without the owner's knowledge, long after an active investigation, to allow for appeals, lawsuits, etc. Congress has countered with legislation of its own, versions of a bill named SAFE (Security and Freedom through Encryption Act) which affirms the right to encrypt digital communications and prohibits mandatory key escrow systems.

In the volatile national security landscape of the 21st century, with simmering or active hostilities in every continent and weapons of mass destruction available in many countries, the ability to clandestinely observe the activities of hostile nations and groups is critical for the government's interest.

Encryption is required for business transactions over the Internet. However, until recently the government felt that high-bit key encryption algorithms could seriously imperil national security. The government responded to rapid encryption developments by regulating encryption as munitions or arms sales. The U.S. government tightly regulated encryption technologies from 1996 until January 2000, when regulations were considerably loosened. Until January 2000, 64-bit mass market products, 56-bit encryption items and 512-bit key management products were listed on the U.S. Munitions List and covered by the International Traffic in Arms Regulations (ITAR).

Industry complaints were strong. U.S. companies pointed out, among other things, that other countries were developing and freely exporting high bit encryption technologies. Also, international commerce was becoming difficult and less secure because high-bit encryption technologies could not be shared with foreign-owned and operated businesses. Export regulations were considerably eased in January 2000, at which point these technologies could be exported to any country except the seven terrorist sponsoring countries (Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria). Among other provisions, high-bit open source encryption, where the source code was freely distributed over the Internet, could be distributed without Department of Commerce review as long as

the Department was notified via email of the URL where the software was available.

At least one analyst (Wilson, 1996) feels that part of the government's concern with encryption is that it will be so widely adopted for foreign intelligence communications that the United States' considerable investment in electronic surveillance tradecraft will be immediately obsolete. (2) There is also a concern that the federal government will have to divert considerable time and resources from other security issues to cryptoanalysis—the discovery, monitoring and breaking of encryption algorithms in use by hostile countries and groups. Other analysts feel, however, that the government, particularly agencies responsible for national security and defense, will rely more heavily on surveillance technologies to intercept communications before or after the encryption process, such as capturing screen displays, when the communication is still in plaintext. Blaine Burnham, Director of Georgia Tech's Information Security Center, notes that every time a new security technology is developed, the government reacts with concern but that as the technology becomes better understood, the government finds acceptable ways of continuing its business of surveillance and interception. He believes that encryption technologies will be no exception. (3)

Questions for Discussion:

1. The federal government under President Clinton favors key escrow and recovery, so that the government has clandestine access to any keys needed to decrypt information in a surveillance situation. If the government must request the key from the key owner, the key owner has the opportunity to alter or delete data to hide evidence of a crime. However, a key escrow system provides a single point of vulnerability for criminals and terrorists seeking access to encrypted information. Industry critics of government key escrow plans have expressed serious concerns about the government's ability to protect a key escrow system from attack. Do you feel the benefits of swift access by government law enforcement to encrypted information outweighs the vulnerabilities of a key recovery program?

2. Although much attention has been given to government intrusion on privacy, particularly for encrypted information, less attention has been paid to violations of privacy by electronic commerce companies, who track consumer purchases and visits to websites and sell that information to niche marketers. Blaine Burnham, Director of the Georgia Tech Information Security Center, cites a California judge who feels that personal information has marketable, commercial value and that property laws should apply rather than privacy laws, to provide legal safeguards and remedies for the consumer. Use of personal information without the owner's permission could thus conceivably be theft. Do you feel this is a useful interpretation or should government sanctions stronger than current property laws be used to control information

misuse? Or, conversely, do you see unconstrained commercial trafficking in personal information as a minor annoyance, similar to junk mail from mailing lists sold by one organization to another?

3. The Internet provides tremendous facilities for collecting information about individuals. Books purchased online, websites visited, conversations on discussion lists and chat lines, can develop a seemingly comprehensive picture of a person. What can you deduce about a person, with a university email address, who has done the following: visited Anti-Online (Hacker website), particularly the virus discussion and download sections, downloaded The Turner Diaries (popular fringe group manifesto, advocating overthrow of the government), studied smallpox on the CDC Emerging Diseases web site, visited the Hizbollah website (Iranian propaganda website), among many other online activities? . Should the person being investigated have the right to examine and challenge this Internet activity record? Should this person be denied a government position requiring a high-level security clearance, for example, if these Internet activities came to light in a routine security check? On what basis should any of this Internet activity be available to the security checker? Who is responsible for the accuracy of that information? (The person in question was researching information for this web page).