Statement of Louis J. Freeh, Director, FBI, before the Senate Judiciary Committee Hearing on Encryption, United States Senate, Washington, D. C. - July 9, 1997 Source: http://WWW.FBI.GOV/congress/encrypt2/encrypt2.htm

Mr. Chairman and members of the committee, I appreciate the opportunity to discuss the issue of encryption and I applaud your willingness to deal with this vital public safety issue.

The looming spectre of the widespread use of robust, virtually uncrackable encryption is one of the most difficult problems confronting law enforcement as the next century approaches. At stake are some of our most valuable and reliable investigative techniques, and the public safety of our citizens. We believe that unless a balanced approach to encryption is adopted that includes a viable key management infrastructure, the ability of law enforcement to investigate and sometimes prevent the most serious crimes and terrorism will be severely impaired. Our national security will also be jeopardized.

For law enforcement, framing the issue is simple. In this time of dazzling telecommunications and computer technology where information can have extraordinary value, the ready availability of robust encryption is essential. No one in law enforcement disputes that. Clearly, in today's world and more so in the future, the ability to encrypt both contemporaneous communications and stored data is a vital component of information security.

As is so often the case, however, there is another aspect to the encryption issue that if left unaddressed will have severe public safety and national security ramifications. Law enforcement is in unanimous agreement that the widespread use of robust non-key recovery encryption ultimately will devastate our ability to fight crime and prevent terrorism. Uncrackable encryption will allow drug lords, spies, terrorists and even violent gangs to communicate about their crimes and their conspiracies with impunity. We will lose one of the few remaining vulnerabilities of the worst criminals and terrorists upon which law enforcement depends to successfully investigate and often prevent the worst crimes.

For this reason, the law enforcement community is unanimous in calling for a balanced solution to this problem. It is called "key recovery" encryption and, in our view, any legislative approach that does not achieve such a balanced approach seriously jeopardizes the long-term viability and usefulness of court-authorized access to transmitted as well as stored evidence and information. Electronic surveillance and

search and seizure are techniques upon which law enforcement depends to ensure public safety and maintain national security.

Under one type of key recovery approach, a decryption "key" for a given encryption product is deposited with a trustworthy key recovery agent for safe keeping. The key recovery agent could be a private company, a bank, or other commercial or government entity that meets established trustworthiness criteria. Should encryption users need access to their encrypted information, they could obtain the decryption key from the key recovery agent. Additionally, when law enforcement needs to decrypt criminal-related communications or computer files lawfully seized under established legal authorities, they too, under conditions prescribed by law and with the presentation of proper legal process, could obtain the decryption key from the key recovery agent. This is the only viable way to permit the timely decryption of lawfully seized communications or computer files that are in furtherance of criminal activity. The key recovery information would be provided to the law enforcement agency under very strict controls and would be used only for its intended public safety purpose. Under this approach, the law-abiding would gain the benefits of strong, robust encryption with emergency access capabilities and public safety and national security would be maintained--as manufacturers produce and sell encryption products that provide key recovery.

This solution meets industry's information security and communications privacy needs for strong encryption while addressing law enforcement's public safety needs for timely decryption when such products are used to conceal crimes or impending acts of terrorism or espionage.

Some have argued that government policy makers should step aside and let market forces solely determine the direction of key recovery encryption, letting market forces determine the type of technologies that will be used and under what circumstances. They argue that most corporations that see the need for encryption will also recognize the need for, and even insist on, key recovery encryption products to secure their electronically stored information and to protect their corporate interests should an encryption key be lost, stolen or used by a rogue employee for extortion purposes.

We agree that rational thinking corporations will act in a prudent manner and will insist on using key recovery encryption for electronically stored information. However, law enforcement has a unique public safety requirement in the area of perishable communications which are in transit (telephone calls, e-mail, etc.). It is law enforcement, not corporations, that has a need for

timely decryption of communications in transit. There is extraordinary risk in trusting public safety and national security to market forces that rightfully are protecting important but unrelated interests. Law enforcement's needs will not be adequately addressed by this type of an approach.

It is for this reason that government policy makers and Congress should play a direct role in shaping our national encryption policy and adopt a balanced approach that addresses both the commercial and the public safety needs. The adverse impact to public safety and national security associated with any type of "wait and see" or voluntary market force approach would be far too great of a price for the American public to pay.

Several bills have recently been introduced which address encryption. Language in some of the proposed bills makes it unlawful to use encryption in the furtherance of criminal activity and set out procedures for law enforcement access to stored keys in those instances where key recovery encryption was voluntarily used. One of these bills, S.909, takes significant strides in the direction of protecting public safety by encouraging the use of key recovery encryption through market based incentives and other inducements.

Unfortunately, these legislative proposals still do not contain adequate assurances that the impact on public safety and effective law enforcement of the widespread availability of encryption will be addressed. We look forward to working with you to develop legislative accommodations that adequately address the public safety needs of law enforcement and a balanced encryption policy.

Further, some argue the encryption "genie is out of the bottle," and that attempts to influence the future use of encryption are futile. I do not believe that to be the case. Key recovery encryption products can, with government and industry support, become a standard for use in the global information infrastructure.

No one contends that a key recovery-based encryption policy will prevent all criminals, spies and terrorists from using non-key recovery encryption. But if we, as a nation, act responsibly and build systems and products that support and rely upon key recovery, all facets of the public's interest can be served.

And as this committee knows, export controls on encryption products exist primarily to protect national security and foreign policy interests. However, law enforcement is more concerned about the significant and growing threat to public safety and effective law

enforcement that would be caused by the proliferation and use within the United States of a communications infrastructure that supports strong encryption products but cannot support timely law enforcement decryption. Without question, such an infrastructure will be used by dangerous criminals and terrorists to conceal their illegal plans and activities from law enforcement, thus inhibiting our ability to enforce the laws and prevent terrorism.

Congress has on many occasions accepted the premise that the use of electronic surveillance is a tool of utmost importance in terrorism cases and in many criminal investigations, especially those involving serious and violent crime, terrorism, espionage, organized crime, drug-trafficking, corruption and fraud. There have been numerous cases where law enforcement, through the use of electronic surveillance, has not only solved and successfully prosecuted serious crimes and dangerous criminals, but has also been able to prevent serious and life-threatening criminal acts. For example, terrorists in New York were plotting to bomb the United Nations Building, the Lincoln and Holland Tunnels, and 26 Federal Plaza as well as conduct assassinations of political figures. Court-authorized electronic surveillance enabled the FBI to disrupt the plot as explosives were being mixed. Ultimately, the evidence obtained was used to convict the conspirators. In another example, electronic surveillance was used to prevent and then convict two men who intended to kidnap, molest and then kill a male child.

Most encryption products manufactured today do not provide for timely law enforcement decryption. Widespread use of non-key recovery encryption or communications infrastructure that supports non-key recovery encrnyption use clearly will undermine law enforcement's ability to effectively carry out its public safety mission and to combat ultra-dangerous criminals and terrorists.

This is not a problem that will begin sometime in the future. Law enforcement is already encountering the harmful effects of encryption in many important investigations today. For example:

> Convicted spy Aldrich Ames was told by the Russian intelligence service to encrypt computer file information that was to be passed to them.
>
> An international terrorist was plotting to blow up 11 U.S.-owned commercial airliners in the far east. His laptop computer which was seized during his arrest in Manilla contained encrypted files concerning this terrorist plot.

A subject in a child pornography case used encryption in transmitting obscene and pornographic images of children over the Internet.

A major international drug trafficking subject recently used a telephone encryption device to frustrate court-approved electronic surveillance.

Requests for cryptographic support pertaining to electronic surveillance interceptions from FBI field offices and other law enforcement agencies have steadily risen over the past several years. For example, from 1995 to 1996, there was a two-fold increase (from 5 to 12) in the number of instances where the FBI's court-authorized electronic efforts were frustrated by the use of encryption that did not allow for law enforcement access.

Over the last three (3) years, the FBI has also seen the number of computer related cases utilizing encryption and/or password protection increase from 20 or two (2) percent of the cases involving electronically stored information to 140 or seven (7) percent. These included the use of 56 bit data encryption standard (DES) and 128 bit "pretty good privacy" (PGP) encryption.

Just as when this committee so boldly addressed digital telephony, the government and the nation are again at an historic crossroad on this issue. The International Association of Chiefs of Police, the National Sheriff's Association and the National District Attorneys Association have all enacted resolutions supporting a balanced encryption policy and opposing any legislation that undercuts or falls short such a balanced policy. If public policy makers act wisely, the safety of all Americans will be enhanced for decades to come. But if narrow interests prevail, then law enforcement will be unable to provide the level of protection that people in a democracy properly expect and deserve.

Conclusion

We are not asking that the magnificent advances in encryption technology be abandoned. We are the strongest proponents of robust, reliable encryption manufactured and sold by American companies all over the world. Our position is simple and, we believe, vital. Encryption is certainly a commercial interest of great importance to this great nation. But it's not merely a commercial or business issue. To those of us charged with the protection of public safety and national security, encryption technology and its application in the information age--here at the dawn of the 21st

century and thereafter--will become a matter of life and death in many instances which will directly impact on our safety and freedoms. Good and sound public policy decisions about encryption must be made now by the Congress and not be left to private enterprise. Legislation which carefully balances public safety and private enterprise must be established with respect to encryption.

Would we allow a car to be driven with features which would evade and outrun police cars? Would we build houses or buildings which firefighters could not enter to save people?

Most importantly, we are not advocating that the privacy rights or personal security of any person or enterprise be compromised or threatened. You can't yell "fire" in a crowded theater. You can't with impunity commit libel or slander. You can't use common law honored privileges to commit crimes.

In support of our position for a rational encryption policy which balances public safety with the right to secure communications, we rely on the Fourth Amendment to the Constitution. There the framers established a delicate balance between "the right of the people to be secure in their persons, houses, papers, and effects (today we might add personal computers, modems, data streams, discs, etc.) against unreasonable searches and seizures." Those precious rights, however, were balanced against the legitimate right and necessity of the police, acting through strict legal process, to gain access by lawful search and seizure to the conversations and stored evidence of criminals, spies and terrorists.

The precepts and balance of the Fourth Amendment have not changed or altered. What has changed from the late eighteenth to the late twentieth century is technology and telecommunications well beyond the contemplation of the framers.

The unchecked proliferation of non key recovery encryption will drastically change the balance of the Fourth Amendment in a way which would shock its original proponents. Police soon may be unable through legal process and with sufficient probable cause to conduct a reasonable and lawful search or seizure, because they cannot gain access to evidence being channeled or stored by criminals, terrorists and spies. Significantly, their lack of future access may be in part due to policy decisions about encryption made or not made by the United States. This would be a terrible upset of the balance so wisely set forth in the Fourth Amendment on December 15, 1791. I urge you to maintain that balance and allow your police departments, district attorneys, sheriffs and federal law enforcement authorities to

continue to use their most effective techniques to fight crime and terrorism--techniques well understood and authorized by the framers and Congress for over two hundred years.

I look forward to working with you on this matter and at this time would be pleased to answer any questions.