



Office of the Attorney General
Washington, D. C. 20530

July 18, 1997

Dear Member of Congress:

Congress is considering a variety of legislative proposals concerning encryption. Some of these proposals would, in effect, make it impossible for the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), Secret Service, Customs Service, Bureau of Alcohol, Tobacco and Firearms, and other federal, state, and local law enforcement agencies to lawfully gain access to criminal telephone conversations or electronically stored evidence possessed by terrorists, child pornographers, drug kingpins, spies and other criminals. Since the impact of these proposals would seriously jeopardize public safety and national security, we collectively urge you to support a different, balanced approach that strongly supports commercial and privacy interests but maintains our ability to investigate and prosecute serious crimes.

We fully recognize that encryption is critical to communications security and privacy, and that substantial commercial interests are at stake. Perhaps in recognition of these facts, all the bills being considered allow market forces to shape the development of encryption products. We, too, place substantial reliance on market forces to promote electronic security and privacy, but believe that we cannot rely solely on market forces to protect the public safety and national security. Obviously, the government cannot abdicate its solemn responsibility to protect public safety and national security.

Currently, of course, encryption is not widely used, and most data is stored, and transmitted, in the clear. As we move from a plaintext world to an encrypted one, we have a critical choice to make: we can either (1) choose robust, unbreakable encryption that protects commerce and privacy but gives criminals a powerful new weapon, or (2) choose robust, unbreakable encryption that protects commerce and privacy and gives law enforcement the ability to protect public safety. The choice should be obvious and it would be a mistake of historic proportions to do nothing about the dangers to public safety posed by encryption without adequate safeguards for law enforcement.

Let there be no doubt: without encryption safeguards, all Americans will be endangered. No one disputes this fact; not

industry, not encryption users, no one. We need to take definitive actions to protect the safety of the public and security of the nation. That is why law enforcement at all levels of government -- including the Justice Department, Treasury Department, the National Association of Attorneys General, International Association of Chiefs of Police, the Major City Chiefs, the National Sheriffs' Association, and the National District Attorneys Association -- are so concerned about this issue.

We all agree that without adequate legislation, law enforcement in the United States will be severely limited in its ability to combat the worst criminals and terrorists. Further, law enforcement agrees that the widespread use of robust non-key recovery encryption ultimately will devastate our ability to fight crime and prevent terrorism.

Simply stated, technology is rapidly developing to the point where powerful encryption will become commonplace both for routine telephone communications and for stored computer data. Without legislation that accommodates public safety and national security concerns, society's most dangerous criminals will be able to communicate safely and electronically store data without fear of discovery. Court orders to conduct electronic surveillance and court-authorized search warrants will be ineffectual, and the Fourth Amendment's carefully-struck balance between ensuring privacy and protecting public safety will be forever altered by technology. Technology should not dictate public policy, and it should promote, rather than defeat, public safety.

We are not suggesting the balance of the Fourth Amendment be tipped toward law enforcement either. To the contrary, we only seek the status quo, not the lessening of any legal standard or the expansion of any law enforcement authority. The Fourth Amendment protects the privacy and liberties of our citizens but permits law enforcement to use tightly controlled investigative techniques to obtain evidence of crimes. The result has been the freest country in the world with the strongest economy.

Law enforcement has already confronted encryption in high-profile espionage, terrorist, and criminal cases. For example:

- * An international terrorist was plotting to blow up 11 U.S.-owned commercial airliners in the Far East. His laptop computer, which was seized in Manila, 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.

And this is just the tip of the iceberg. Convicted spy Aldrich Ames, for example, was told by the Russian Intelligence Service to encrypt computer file information that was to be passed to them.

Further, today's international drug trafficking organizations are the most powerful, ruthless and affluent criminal enterprises we have ever faced. We know from numerous past investigations that they have utilized their virtually unlimited wealth to purchase sophisticated electronic equipment to facilitate their illegal activities. This has included state of the art communication and encryption devices. They have used this equipment as part of their command and control process for their international criminal operations. We believe you share our concern that criminals will increasingly take advantage of developing technology to further insulate their violent and destructive activities.

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. There has been an increase in the number of instances where the FBI's and DEA's court-authorized electronic efforts were frustrated by the use of encryption that did not allow for law enforcement access.

There have also been numerous other cases where law enforcement, through the use of electronic surveillance, has not only solved and successfully prosecuted serious crimes but has also been able to prevent 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 stop and then convict two men who intended to kidnap, molest, and kill a child. In all of these cases, the use of encryption might have seriously jeopardized public safety and resulted in the loss of life.

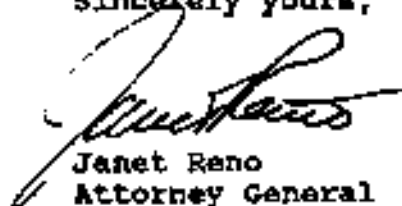
To preserve law enforcement's abilities, and to preserve the balance so carefully established by the Constitution, we believe any encryption legislation must accomplish three goals in addition to promoting the widespread use of strong encryption. It must establish:

- * A viable Key management infrastructure that promotes electronic commerce and enjoys the confidence of encryption users.
- * A key management infrastructure that supports a key recovery scheme that will allow encryption users access to their own data should the need arise, and that will permit law enforcement to obtain lawful access to the plain text of encrypted communications and data.
- * An enforcement mechanism that criminalizes both improper use of encryption key recovery information and the use of encryption for criminal purposes.

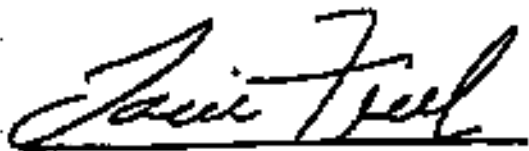
Only one bill, S.909 (the McCain/Kerrey/Hollings bill), comes close to meeting these core public safety, law enforcement, and national security needs. The other bills being considered by Congress, as currently written, risk great harm to our ability to enforce the laws and protect our citizens. We look forward to working to improve the McCain/Kerrey/Hollings bill.

In sum, while encryption is certainly a commercial interest of great importance to this Nation, it is not solely a commercial or business issue. Those of us charged with the protection of public safety and national security, believe that the misuse of encryption technology will become a matter of life and death in many instances. That is why we urge you to adopt a balanced approach that accomplishes the goals mentioned above. Only this approach will allow police departments, attorneys general, district attorneys, sheriffs, and federal authorities to continue to use their most effective investigative techniques, with court approval, to fight crime and espionage and prevent terrorism.

Sincerely yours,



Janet Reno
Attorney General




Louis Frach
Director
Federal Bureau of Investigation



Barry McCaffrey
Director
Office of National Drug
Control Policy



Thomas A. Constantine
Director
Drug Enforcement Administration



Lewis C. Marletti
Director
United States Secret Service



Raymond W. Kelly
Undersecretary for Enforcement
U.S. Department of Treasury



George J. Weisse
Commissioner
United States Customs Service



John W. Magaw
Director
Bureau of Alcohol, Tobacco
and Firearms