"Encryption Standards and Procedures Act of 1994"

HON. GEORGE E. BROWN, JR.

of California

In the House of Representatives

Thursday, October 6, 1994

Mr. Speaker, today I am introducing H.R. 5199, the Encryption Standards and Procedures Act of 1994. The purpose of this legislation is to establish Federal policy governing the development and use of encryption technology for unclassified information that strikes the proper balance between the public's right to private and secure communications and the government's need to decipher information obtained through lawful surveillance.

The legislation would authorize the National Institute of Standards and Technology (NIST) to develop and issue, by regulation, federal encryption standards for ensuring privacy, security, and authenticity of domestic and international electronic communications in a way that preserves privacy rights and maintains the government's authority and ability to conduct electronic surveillance. The development of such standards under a rulemaking process will ensure that all stakeholders have an opportunity to influence the final program. With respect to that policy, the bill would permit wider use of encryption technology while reasserting Fourth Amendment privacy rights and the government's authority to conduct lawful electronic surveillance. To ensure those rights are preserved, the bill would impose new legal requirements on escrow agents that may be part of an encryption standard established under the legislation. It would also establish a research and development program at NIST to develop next generation encryption technology, and would authorize the use of available appropriations to implement the legislation.

Mr. Speaker, this administration has placed a high priority on promoting the National Information Infrastructure (NII) and in realizing fully the economic and social benefits of that infrastructure. To achieve these goals, which I strongly endorse, information communicated over the NII must be secure, private, and authentic. Otherwise, the public will not fully use the NII and we will not realize its vast potential benefits. Encryption technology provides this capability.

During the Cold War, the Federal Government pursued a de facto policy of suppressing private sector development, use, and export of encryption technology for national security reasons. Recent advancements in

encryption technology and its proliferation make enforcement of that policy increasingly difficult. Moreover, fulfilling the goals of the National Information Infrastructure requires private and secure communications that can only be achieved with encryption technology. The widespread use of that technology, however, threatens to impede the government's ability to conduct lawful electronic surveillance.

In February, 1994, the Administration responded to this dilemma by formally adopting a voluntary federal Escrowed Encryption Standard (EES) for electronic voice communications known as "Clipper". The standard would be implemented in computer chips that use a classified mathematical formula to encrypt unclassified telephone conversations and computer data transmitted over public telephone networks. Authorized government agencies can decode those communications by presenting a legal request to two escrow agents, which would hold two halves of a mathematical key that can decipher the code.

The purposes of Clipper are two fold -- first, to provide a means to safeguard public and private electronic voice communications and, second, to enable government law enforcement authorities and intelligence gathering agencies to decipher such coummunications that have been lawfully intercepted. Similar voluntary standards for electronic data communications are under development by the government and may soon be issued. The Administration contends that it has authority under the Computer Security Act to issue such standards. Others, however, have raised concerns about the proper interpretation and application of the Act with respect to Clipper and similar standards.

The Computer Secuirty Act, which the Committee on Science, Space, and Technology reported and the Congress enacted in 1987, authorized NIST, in consultation with other appropriate federal agencies, to develop and issue standards and guidelines for protecting "unclassified, sensitive information" in "federal computer systems". The Act did not explicitly contemplate the development or issuance of standards for safeguarding private communications and satisfying the information needs of law enforcement and the intelligence community. Such communications are considered private property subject to separate and distinct constitutional rights and legal protections. The Administration's interpretation of the Computer Security Act to cover such matters appears to go beyond the original intent of the Act and may be inconsistent with other law pertaining to individual privacy, protection of private property, and government authority to conduct lawful electronic surveillance.

In testimony at hearings before our Committee, witnesses from industry and privacy groups objected to the secretive way Clipper was developed, and stated that the initiative does not go far enough to promote widespread use

of encryption technology. They argued that the program will hamper business opportunities for United States firms, may infringe on individual privacy rights, and is prone to abuse. The Administration refutes these claims and intends to proceed with the initiative arguing that it is essential for public safety and national security. The issue currently is stalemated unless there is legislation or third party intervention.

The Administration has publicly stated that it does not intend to seek legislation expressly authorizing Clipper or any other federal encryption standard because it wants flexibility to modify its encryption policy and program in response to changing circumstances. The Administration's desire for flexibility, however, contributes to the public's mistrust and opposition to Clipper. The proposal was developed under an administrative directive and, therefore, could just as easily be changed in a way that might be construed to diminish privacy rights without giving the public adequate opportunity to affect the program. For this reason alone, the public is unlikely to ever accept Clipper Chip in its present form.

I, along with others, believe that a viable approach to gain public support for an initiative like Clipper is legislation to codify encryption policy and govern how that policy would be implemented. In so doing, all stakeholders would have an opportunity to influence policy. The final program would have been subjected to greater scrutiny and its implementation would be under the rule of law. It may well be that only under these circumstances would the public accept a federal encryption standard and the needs of law enforcement could be satisfied without compromising privacy rights.

The Office of Technology Assessment (OTA) issued in September an extensive report entitled "Information Security and Privacy Network Environments" that is consistent with this view. The report concluded that "appropriate institutional and technical safeguards are required for a broad range of personal ... information, [o]therwise, concerns for the security and privacy of networked information may limit the usefulness and acceptance of the global information infrastructure." OTA also stated that such safeguards can only be developed successfully through an "open process" and with congressional involvement so the views of all affected parties can be considered properly in arriving at a final outcome. Public trust in government and acceptance of federal encryption standards can only be achieved through such a process. This sentiment was shared by most respondents to a draft of the bill circulated earlier this Summer for comments.

Mr. Speaker, the bill I have introduced today has been drafted, not as a perfect solution to the problem of privacy and security in the electronic information age, but as a means for getting the various factions to talk to

each other in an open process to reach a sensible and effective resolution of this critical issue. I invite all interested parties to comment on the bill. My intention is to modify the bill to reflect comments made and to introduce it again early in the 104th Congress for consideration by this body.