The Clipper chip proposal was contested by groups like the Electronic Frontier Foundation and the Electronic Privacy Information Center, which claimed that it would result in citizens being subjected to more extensive and possibly unlawful government surveillance.Secure mobile devices and smartphone applications exist, but they may require specialized hardware and typically require both parties to the communication to use the same encryption mechanism.Clipper's escrow system had a serious security flaw when the chip sent a 128-bit "Law Enforcement Access Field" (LEAF) containing the information needed to recover the encryption key. To prevent the message from being altered by the program that sent it, a 16-bit hash was added to the LEAF. The Clipper chip would not decrypt a message with an invalid hash, but the 16-bit hash was too short to provide any practical security. After the attempt at escrow, a brute force attack would quickly produce a new LEAF value that would yield the same hash but the incorrect keys. This would prevent the key from being escrowed and enable the Clipper chip to be used as an encryption device. To circumvent the real-time escrow, Yair Frankel and Moti Young published another design-based attack in 1995 that demonstrated how a device's key escrow tracking and authentication capability (LEAF) could be attached to messages from another device and still be received. A group of top cryptographers examined the architectural flaws in key escrow implementations generally, including but not limited to the Clipper chip Skipjack protocol, in their 1997 paper "Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption.Government pressure to obtain the Clipper chip led to the development and release of several powerful encryption software programs, such as Nautilus, PGP, and PGP fone.