CEI ON POINT

The Competitive Enterprise Institute
1001 Connecticut Avenue NW • Suite 1250 • Washington, D.C. 20036 • (202) 331-1010 • http://www.cei.org
Advancing the Principles of Free Enterprise and Limited Government

July 7, 1999 No. 42

The SAFE Bill: Keying in on Encryption Reform

By Ananda Gupta[1]

Despite Clinton Administration steps towards liberalizing American encryption policy, some members of the House of Representatives have rightly decided that it hasn't gone far enough. Accordingly, Reps. Bob Goodlatte (R-VA) and Zoe Lofgren (D-CA) re-introduced the SAFE bill (Security And Freedom through Encryption, H.R. 850), early this year. SAFE would reform current U.S. crypto policy in a number of important ways, primarily by removing arbitrary limits on encryption key lengths. Rep. Goodlatte is optimistic about committee action on the bill as early as this month, as SAFE passed the Commerce Committee this week.

How encryption works. Encryption is the technique of translating readable (or "plaintext") messages into unreadable code, by way of a mathematical formula. An encryption program's "strength" depends not just on the formula but on the length of the "key" which unlocks the code and decrypts the message. Under "public key" or "dual-key" encryption schemes, each user has two keys, a public one and a private one.

So, when John wants to send a message to Jane for her eyes only, he can look up her public key in a directory or on her Web page and use it to encrypt his message. She receives the message and uses her private key (known only to her) to decrypt it – anyone else's private key would result in the message appearing as gibberish. So, as long as Jane has not let anyone else know her private key, the message is secure.

The "strength" of a key-based encryption system depends on the length of the keys, which become exponentially more difficult to "break" as they get longer. Each digit in a key is either a "1" or a "0" – so, for example, there are only four possible 2-bit keys: 11, 01, 10, and 00. Needless to say, a message encoded with a 2-bit key is not very secure – a snooper would only need to try those four sequences, since the key would have to be one of them.

The current policy. Current law regulates encryption by strength – that is, the key length accommodated by a crypto program partly determines what rules it must obey. Until last year, 56-bit (and stronger) keys were export-restricted; they could only be sold or sent to foreign subsidiaries of U.S. firms, or to foreign governments within a particular policy portfolio. Now, the restrictions have been loosened so that 80 bits is the new threshold – any product stronger than 80 bits now labors under those restrictions.

---

[1] Ananda Gupta (agupta@cei.org) is research assistant at the Competitive Enterprise Institute.

SAFE would eliminate specific key lengths from the regulations, allowing consumers and firms to employ unlimited-length keys without waiting for bureaucrats to react to their standards' discredit. Such lack of specificity is good because the benchmark of true security increases. It is likely that even the new standard, 80-bit, will be broken before the year 2000. Americans and foreign buyers of American products should not have to jump through slowly-revised federal hoops before they upgrade their security.

Moreover, export controls chill domestic development, since it is easier for a firm to produce and distribute a single, weak version rather than a strong domestic version and a weak, regulation-passing export version. In fact, some firms have ceased operating in the U.S., taking advantage of their product's intangibility and incorporating in countries without encryption regulation. Hush Communications, for example, recently launched a new service – free encrypted email – in April. But they did so from the British West Indies.

SAFE only goes so far to relieve this burden, allowing firms to export their products freely when a comparable foreign product is *already* available. This allows U.S. cryptography products of varying strengths to hit foreign markets, but ensures that they will be second to market – an unnecessary and possibly disastrous restriction, especially when brand-switching requires a user to learn a new program.

The real prize. More fundamentally than its economic effects, SAFE would remove an obstacle to one of Americans' most cherished prerogatives – being left alone. Encryption allows even the relatively computer illiterate to keep their business and affairs to themselves. In a free society, allowing the market to provide such a service should go without saying.

The law enforcement community, especially at the federal level, distrusts encryption because it fears encryption will interfere with the monitoring schemes it uses to catch criminals (primarily drug offenders). To soothe them, SAFE also imposes criminal penalties for using encryption to conceal evidence in a crime. But that's unlikely to satisfy the Federal Bureau of Investigation and other law enforcement agencies, who are accustomed to nearly limitless wiretap and other monitoring authority. Nonetheless, since telephone wiretaps are disproportionately used to gather evidence in drug and vice cases, not the emotional, headline-grabbing cases of terrorism or murder, it's unlikely that Americans will want to give up more of their privacy and personal security just to keep one more pot dealer off the streets.

In any case, there is no reason why the FBI should be exempted from law enforcement innovation. Wiretaps themselves arose as a response to the telephone; no doubt many pre-telephone agents would have been just as happy had there never been a telephone. Imagine criminals' being able to talk to one another over great distances!

Conclusion. In short, SAFE still unnecessarily hamstrings U.S. firms by forcing them to follow in their foreign competitors' footsteps when it comes to opening markets abroad. That is the argument cited most often by Rep. Goodlatte and other SAFE supporters in Congress. But SAFE's abolition of arbitrary key-length standards and its implied affirmation of Americans' right to encrypt their communications with whatever products they see fit are bold steps in the right direction, and will affect far more than just the bottom line.