International Bulletin of Political Psychology

Volume 3 | Issue 4 Article 3

8-22-1997

Trends. Encrypting Encryption: Some Comments on S. 909, Secure Public Networks Act

IBPP Editor
bloomr@erau.edu

Trends. Encrypting Encryption: Some Comments on S. 909, Secure Public Networks Act

Cover Page Footnote

The author discusses the main purpose of S. 909--the Kerrey-McCain bill--which is to render it more difficult for technology and telecommunications to be employed by people in the commission of crimes.

International Bulletin of Political Psychology

Title: Trends. Encrypting Encryption: Some Comments on S. 909, Secure Public Networks Act
Editor: Editor
Volume: 3
Issue: 4
Date: 1997-08-22
Keywords: Encryption, Key Recovery Agent, Security

A main purpose of S. 909--the Kerrey-McCain bill--is to render it more difficult for technology and telecommunications to be employed by people in the commission of crimes, viz., terrorism and organized crime. The bill advocates a key recovery plan that will require almost all users of encryption to provide a copy of every key they use to so-called key recovery agents. An agent--with proper authorization--will facilitate access for law enforcement or other political authorities--with proper authorization--to the so-called plaintext of requested communications

Much already has been written about the technical, conceptual, cost, legal, and political problems of key recovery plans. Interestingly, the same Issues accompanying counter-encryption efforts from early in human history are still as salient in assessing the merits of S.909 and similar initiatives.

(1) Encryptors engaged in crime may change how they protect information in response to a well-publicized effort. They will no longer employ that which is now vulnerable and often will protect information about this change of information from the counter-encryptors. This results in wasted assets for the counter-encryptors. (2) The actual meaning of a message or the message itself that is sought by the counter-encryptors may be as plain as day but unrecognized respectively as meaning or message. The encryptors may choose to use symbols, signs, patterns, images, words, or movements among other modes to convey the sought meaning. All the key recovery agent can offer is the so-called plaintext. (3) The greater the restrictions placed on encryption, the less likely encryption and encryption breakthroughs can occur to aid legitimate pursuits. And these legitimate pursuits are themselves often impediments to successful crime. As well, as restrictions increase, the more opportunities for illegal provision of encryption measures that lead to increases in crime and subversion of established legal and political authority. (4) Key recovery plans do not prevent those who circumvent regulation from using encryption for criminal purposes. (Of course, at this point all people who don't comply with regulation automatically become criminals.) (5) Apocryphal keys can be created to yield apocryphal messages while seeming to comply with regulation. (6) Proponents of counter-encryption programs often promise more than can be feasibly delivered because of technological or cost problems. (Remember the Strategic Defense Initiative?) (7) Human weakness will make all regulatory schemes vulnerable--e.g., through bribery, sabotage, theft, fatigue, and problems in judgment. (8) The low base rate of what legal and political authorities might be after may not justify the imposition on so many law-abiding citizens.

These Issues are not necessarily insurmountable in legitimate attempts to provide security. But, too often, they become detached from the purely technical aspects of encryption. In essence, at this point encryption becomes encrypted. (See Bill Summary and Status for the 105th Congress, S.909, http://thomas.loc.gov/cgi-bin/bdquery/z?d105:SN00909:@@@L; Press Release on Electronic Surveillance-Report of the FBI's Publication of the Second Notice of Capacity, January 14, 1997, http://www.fbi.gov; Speech by Louis J.. Freeh, Director of the Federal Bureau of Investigation, International Computer Crime Conference, March 4, 1997.) (Keywords: Encryption, Key Recovery Agent, Security)