

SAN DIEGO Jewish World

Volume 2, Number 219

"There's a Jewish story everywhere"

Thursday, September 11, 2008

Remembering 9/11/2001

GUEST COLUMN

Does government need 'back door' authority to break encryption codes?

By Martin Charles Golumbic



HAIFA, Israel—Cyber-terrorists are after data, everything from military communications to national defense secrets. We can lock up this data with technology tools called encryption, a word of ancient Greek etymology meaning secret writing. But what happens when encryption tools, which are readily available on the open market, are used by hostile groups to shield activities from the government's eyes? Should we regulate the use of encryption programs (even if we could?)

The widespread availability of encryption means that investigators encounter difficulties in accessing information necessary for law enforcement and security purposes. The stronger the encryption products, the more difficult it is for law enforcement agencies to gather information about terrorists and their plans. And if we did regulate such programs, how would companies producing new and innovative products be sure that their industrial secrets weren't leaked? For encryption also helps ensure such activities as the secrecy of online payments and the protection of copyrighted music against unauthorized use. We hold dear the right to develop ideas, market them, and make money from them. What kind of chilling effect would the lack of secure communications have on research and development in both the private and the public sectors?

The threat of information warfare demands a reconsideration of the regulation of encryption products. From an economic standpoint, the question is whether terrorist activities concealed by encryption and the breaking of encryption by hostile elements constitute market failures justifying regulatory intervention.

Regulation needs to take into account the extreme cases in society, not the innocent citizen, but the terrorist, who uses electronic communications and other methods protected by encryption. Governmental authorities need a kind of “back door” key to break into them. A 1994 law does require that the software design enable the government to access call-identifying information and allow the transmission of intercepted information to the government. But giving the government “back-door” control can result in both direct harm and indirect damages. It is crucial, therefore, to promote and encourage ongoing dialogue between the technology innovators and the guardians of the legal world. It may not be important for the latter to understand the mathematical details of a particular encryption system, but they should understand the limits to which the various levels of privacy and security can be guaranteed. Law-making and its enforcement demand the convergence of security, technology, and the law.

New legal regulations must be formulated with the characteristics of the Internet in mind. The application of checks and balances to the Internet requires formulating a definition of the circumstances that require the deletion of existing files, the prevention of recording information, and restrictions on saving data. An explicit, narrow general arrangement regarding encryption may be effective in limiting the indirect damage done to privacy. The failure to provide law enforcement agencies with sufficient means of decryption (“back-door” access) or the establishment of overly rigid criteria and procedures for obtaining permission for specific decryption operations could bring about an undesirable result in the form of less focused surveillance. Prior judicial review is essential: any authority that requests the use of “back-door” penetration or any other means of breaking encryption should apply to the court prior to doing so. The extent of the government’s intervention in the production and importation of technological measures needs to be defined, as does the extent to which the state is entitled to obtain access to “back doors.”

In Israel, the determination of policy in regard to encryption is carried out by the executive branch without the direction of the legislature. From the point of view of the principles of administrative and constitutional law, this arrangement is highly problematic, with negative implications. Any system of regulation, ranging from total exemption for civilian products to regulation (such as export restrictions) for products with a defense or security orientation, needs to be based on the characteristics—and different uses—of the products in question and the functions they are supposed to fulfill.

The law must clearly and explicitly define the extent of the regulation and the boundaries of the government’s discretion. A possible model is to permit registration of encryption products without imposing prior control—this would place a single obligation on the producers of an encryption product: registration of its existence and the provision of general information about the product. This would allow the government to be aware of products on the market and of their producers, and to apply to the courts for permission to investigate should a need arise.

Martin Charles Golumbic, a computer scientist and senior professor, is Director of the Caesarea Rothschild Institute at the University of Haifa in Israel, and author of "Fighting Terror Online: The Convergence of Security, Technology and the Law"



<http://www.springer.com/978-0-387-73577-1>

Fighting Terror Online

The Convergence of Security, Technology, and the Law

Golumbic, M.C.

2008, XIV, 178 p., Hardcover

ISBN: 978-0-387-73577-1