

UNLIKELY ADVERSARIES: THE BUSINESS AND LAW ENFORCEMENT COMMUNITIES

*Ronald K. Noble**

Businesses need access to encryption technology in order to maintain growth. Internet use is growing exponentially. As more people are able to afford computers, their desire to use the Internet to purchase products is also growing. In 1996, sales of goods on the Internet exceeded \$500 million, and this figure is expected to exceed \$6.6 billion by the year 2000.¹ The Internet is estimated to have contributed \$200 billion to the economic output of the United States.² It is also estimated that the Internet is responsible for 760,000 new jobs or 50 percent of all new jobs created in the United States in 1996.³ Because on-line consumers have requested security to ensure that their basic credit card purchases are protected, the need for quality encryption technology is essential for businesses to survive. Therefore, the business community is an outspoken proponent of lessening requirements on encryption. Furthermore, businesses state that unless a change is made in the cryptography policy of the United States, U.S. dominance in the emerging information economy will ultimately be placed in jeopardy.

The other side of our contrast involves law enforcement. Law enforcement has a duty to protect national security and domestic tranquility. The Drug Enforcement Administration is seeking ways to deal with encrypted drug trafficking messages, which have increased

* Professor of Law and Faculty Director of the Root-Tilden-Kern Scholarship Program, New York University School of Law.

1. See *The Emergence of a Networked World: Commerce, Society and the Future of the Internet*, GLOBAL INTERNET PROJECT (visited Oct. 21, 1999) <<http://www.gip.org/gip2b.htm>>. At the time of publication, this projection for the year 2000 had, in fact, already been exceeded by estimates for 1998 on-line retail trade. See DAVID HENRY ET AL., U.S. DEP'T OF COMMERCE, *THE EMERGING DIGITAL ECONOMY* (visited Oct. 25, 1999) <<http://www.ecommerce.gov/ede/chapter1.html>> (to be released in printed format in July 2000).

2. See Takuma Amano & Robert Blohm, *The Internet and the Economy*, GLOBAL INTERNET PROJECT (visited Oct. 21, 1999) <<http://www.gip.org/gip9e3.htm>>.

3. See *id.*

from seven to over 250 in just one year alone.⁴ Similarly, the Federal Bureau of Investigation (FBI) is searching for methods to combat the risk of terrorists using encryption to bypass regular intelligence efforts. In response to these concerns, the FBI, Secret Service, and other agencies have taken a strong stance in favor of granting law enforcement the same access to de-encryption technology that they currently have for the purposes of installing wire taps and the like.⁵

4. Cf. LABORATORY DIVISION, FED. BUREAU OF INVESTIGATION, ENCRYPTION: IMPACT ON LAW ENFORCEMENT 7 (1999) (“The CART has seen the number of cases utilizing encryption and/or password protection increase from two (2) percent to approximately twenty (20) percent over the past four years . . .”).

5. Incidentally, both the business and law enforcement communities recognize that encryption keys may be dangerous. Even if we can trust our own police, reciprocity between the United States and foreign governments might place powerful tools for stealing industrial secrets into the hands of foreign countries, some of which are known or at least believed to engage in business espionage. See James Gordon Meek, *G-Man Warns of Foreign Industrial Espionage*, APB NEWS (Oct. 6, 1999) <http://www.apbnews.com/newscenter/internetcrime/1999/10/06/y2k1006_01.html>.