

Economic espionage forced Ellery Systems, Inc. out of business and robbed the U.S. of a competitive advantage in an emerging high-tech industry.

Espionage Killed the Company

The United States lost competitive advantage in a strategically important emerging industry when a Chinese citizen employee of Ellery Systems, Inc. resigned and took with him computer software source codes. The codes had cost \$950,000 to produce and had a potential market value of tens of billions of dollars.

As a direct result of this loss, Ellery Systems, Inc. went out of business and 25 employees lost their jobs. Man-centuries of incredibly complex and hard work and millions of dollars of investment were lost to a foreign country.

Technically, one can't say the software codes were "stolen," as that was never proven in court despite an **arrest, confession and ample independent evidence collected by the FBI.** Prosecution had to be dropped and the Ellery Systems employee went free because the United States did not, at that time, have an effective law for the prosecution of economic espionage. According to Robert Bryant, then head of the FBI's National Security Division, lack of industrial espionage laws hamstrung hundreds of FBI investigations involving the intelligence services of at least 23 countries, half of them unfriendly states and the rest friends and close allies.

Thanks in part to the high-profile Ellery Systems case, that gap in U.S. law was remedied in 1996 with passage of the Economic Espionage Act.

Ellery Systems, a small, entrepreneurial company in Boulder, CO, was at the forefront of building the much-heralded information superhighway. It's specialty, called Distributed Computing Technology, provides a link between major telecommunications technologies and computing. Department of Defense funded the early development of Ellery's technology for intelligence and C3I applications. Ellery was providing specialized software to NASA and working on developing a library of innovative applications for business and other markets.

A Chinese employee of Ellery had, with the knowledge of Ellery's management, recently gone to China to "visit his sick mother." Within days of his return, this employee submitted his resignation. The following day, the software source code for Ellery's products was downloaded via the Internet to a Chinese friend of this employee at a software development company in Denver known to have Chinese connections. The Chinese employee allegedly received \$550,000 from a Chinese government-controlled export-import corporation to set up his own software development firm in the United States to compete with Ellery Systems.

FBI agent John Gedney reportedly told the judge the alleged theft of the software source code fits a profile "of Chinese intelligence operations."

The Chinese employee was a citizen of the People's Republic of China who had been in the United States for five years. During the Chinese government crackdown on pro-democracy demonstrators in Tienanmen Square, he had joined a protest in Denver of the Chinese action. American friends were surprised by his arrest. They said he liked his job at Ellery Systems, attended church, and enjoyed his freedom so much he wanted to gain U.S. citizenship. They had never had any reason to doubt his honesty and integrity.

According to Geoffrey Shaw, former Chief Executive Officer of Ellery Systems in testimony before Congress, the former employee and his Chinese friend admitted taking Ellery systems' source code. They admitted meeting with government and company officials from the People's Republic of China to set up a company to use the technology taken from Ellery to produce applications and other products. They admitted entering into an agreement to provide this technology to a Chinese company in return for money. They admitted deleting copyright notices and other identifiers that would indicate the software codes were clearly Ellery Systems' property. And they admitted lying to Ellery Systems officials when asked if they were in possession of any property of Ellery Systems.

As noted above, prosecution had to be dropped because, at that time, no federal statute directly addressed economic espionage or the protection of proprietary economic information. This was remedied soon thereafter by the Economic Espionage Act of 1996.

The National Counterintelligence Center has prepared a video, entitled *Risky Business*, based largely on the Ellery Systems case.

References

1. Testimony by Geoffrey Shaw, former Chief Executive Officer of Ellery Systems, Inc., before a joint session of the U.S. Senate Select Committee on Intelligence and the Subcommittee on Terrorism, Technology and Government Information of the Senate Judiciary Committee, February 27, 1996. Stephen Keating, "Global Intrigue on Info Highway, Local Case Alleges Chinese Piracy," *The Denver Post*, April 24, 1994, p. A-1.
2. Jonathan Landay, "Congress Moves to Stop Spies in the Workplace," *The Christian Science Monitor*, March 12, 1996, p. 1.
3. "Technology Theft Suspect Remains Under House Arrest," *Reuters*, April 15, 1994.