

- ell, D. (December, 2004). Beyond offshoring: Assess your company's global potential. *Harvard Business Review*, 82-90.
- ell, D. (June, 2006). Smarter offshoring. *Harvard Business Review*, 85-89.
- erman, C. (2007). *The Wal-Mart effect*. New York: Penguin Group.
- F. X. (November, 2006). Breaking the trade-off between efficiency and service. *Harvard Business Review*, 93-212.
- nov, F., & Izraeli, O. (Jan/Feb, 2012). How much inequality is necessary for growth? *Harvard Business Review*, 90(1/2), 8.
- er, T. (2011). Rebooting their systems. *Economist*, 398(8724), 73-74.
- hheim, R., & Lacity, M. (February, 2000). The myths and realities of information technology insourcing. *Communications of the ACM*, 43(2), 99-107.
- ey, B. (October, 2007). Offshoring in reverse. *Industry Week*, 256(10), 41-43.
- l. (February, 2012). Congress moves to cut off off-shoring. *CRM Magazine*, 16(2), 15.
- ring in obscurity. (1994). *Economist*, 332(7881), 74.
- P. T. (January 16, 2012). Closer to near-sourcing. *Journal of Commerce*, 13(2), 8-11.

International Trade Secret Protection: Global Issues and Responses

William M. Fitzpatrick, Villanova University
Samuel A. DiLullo, Villanova University

EXECUTIVE SUMMARY

Trade secrets represent a major source of economic value and competitive advantage for firms. These IPs have been actively targeted by individuals, organizations and nations through economic espionage. In response to this espionage, many countries have sought to develop laws protecting trade secrets. Unfortunately, on an international basis, these country-level responses to trade secret misappropriation have been characterized by inconsistencies in both legal protection/enforcement. This paper provides a select review of these country-level and international responses to trade secret protection. The BELTS paradigm is developed in order to assist organizations in proactively protecting their trade secrets in international commerce.

Keywords: Trade secrets, Economic espionage, Trade secret misappropriation

INTRODUCTION

Hanjuan Jin, a naturalized American citizen and software engineer, was employed by *Motorola Corporation* in the United States. Between June and November of 2006, she requested and was granted a medical leave of absence from the corporation. While on this medical leave, Ms. Jin traveled to the People's Republic of China (PRC) and sought employment with the Chinese telecommunications firm *Sun Kaisens*. Pursuant to this employment, Ms. Jin assisted *Sun Kaisens* in the development of telecommunications products for the PRC military. Returning to the United States in February of 2007, Jin informed *Motorola* that she was prepared to resume her software engineering activities. However, Jin failed to inform this U.S. employer of her intent to return to China and continue her work for *Sun Kaisens*. Upon reporting to work on February 26, 2007, Ms. Jin subsequently accessed *Motorola's* secure internal computer network and downloaded hundreds of documents containing technical data and trade secrets associated with the company's proprietary iDEN telecommunications technology.

February 28, 2007, Ms. Jin was intercepted by agents of both the *FBI* and *U.S. Customs and Border Protection* as she attempted to return to the PRC. In her possession were *Motorola* trade secrets and classified documents revealing her work and development activities for the Chinese military. Hanjuan Jin was both charged with violations of the *Economic Espionage Act* (1996) and subsequently convicted of trade secret theft. She was sentenced to four years of imprisonment in August 2012 (U.S. Department of Justice, 2013).

Trade secret theft or misappropriation has become both an illicit conduit for technological innovation among corporations/nation states (Pacini & Placid, 2009; Carr & Gorman, 2001) and a major source of financial loss for inventive organizations (Almeling, 2012). Since the mid 1990s, 57 countries have been identified as implementing economic espionage activities in order to uncover and exploit the trade secrets of American businesses. These countries include China, Russia, Cuba, Israel, Iran, Japan, India and many European trading partners of the United States (Schweizer, 1996; Carr & Gorman, 2001; Pacini & Placid, 2009). In recent years, industry studies have revealed that losses due to trade secret misappropriation cost U.S. firms \$300 billion annually (Almeling, 2012; ASIS, 2007; Marsh, 2013). Proprietary information losses, attributable to cyber-attacks, have topped \$1 trillion/year on a global basis and also account for significant job losses in the world economy (Almeling, 2012, Marsh, 2013; McAfee, 2009).