Introduction

The United States Congress enacted the Economic Espionage Act (EEA)[1] in 1996, in the midst of a radical transformation of the world's economy. In the twentieth century, the United States became an economic superpower by virtue of its manufacturing prowess—i.e., the use of physical capital to convert resources into goods demanded by the market. By the end of the century, however, the revolution in information technology had wrought a fundamental change in the nature of the United States' economy—and the world's. As one author put it, in the "information age:"

> Ownership of physical capital . . . once the heart of the industrial way of life, becomes increasingly marginal to the economic process. . . . Intellectual capital, on the other hand, is the driving force of the new era, and much coveted. Concepts, ideas and images—not things—are the real items of value in the new economy. Wealth is no longer vested in physical capital but rather in human imagination and creativity.[2]

A 2007 report concluded that "as much as 75 percent of most organizations' value and sources of revenue (or wealth) creation are in intangible assets, intellectual property, and proprietary competitive advantages"[3] One study reported that intangible assets such as trade secrets, which had comprised 17 percent of the total value of the S&P 500 companies in 1975, had grown to 68 percent of that value by 1995, and 81 percent by 2009.[4]

1. 18 U.S.C. §§ 1831–1839.
2. Jeremy Rifkin, The Age of Access 5 (Putnam 2000).
3. *Trends in Proprietary Information Loss*, ASIS International 37 (Aug. 2007), *available at* https://foundation.asisonline.org/FoundationResearch/Publications/Documents/trendsinproprietaryinformationloss.pdf; *see also* Forrester Consulting, The Value of Corporate Secrets 5 (Mar. 2010), *available at* https://www.nsi.org/pdf/reports/The%20Value%20of%20Corporate%20Secrets.pdf (concluding, based on survey of North American, European, Australian, and New Zealand companies, that "[e]nterprises in highly knowledge-intensive industries like manufacturing, information services, professional, scientific and technical services, and transportation accrue between 70% and 80% of their information portfolio value from secrets").
4. David S. Almeling, *Seven Reasons Why Trade Secrets Are Increasingly Important*, 27 Berkeley Tech. L.J. 1091, 1093 (2012) (citing James H. Malackowski, *The Intellectual Property Marketplace Past, Present and Future,* 5. J. Marshall Rev. Intell. Prop. L. 605, 611 (2006)).

Like anything else, as information becomes valuable, it attracts thieves,[5] and by 1996, it was estimated that nearly $24 billion of corporate intellectual property was being stolen each year.[6] In enacting the EEA, Congress cited a 1995 survey in which nearly one-half of corporate respondents reported having experienced a trade secret theft.[7] By 2011, the security firm McAfee reported that "every company in every conceivable industry with significant size and valuable intellectual property and trade secrets has been compromised (or will be shortly)."[8]

In addition to their increased value, other changes also contributed to the attractiveness of trade secrets to thieves. Most importantly, technology has made their theft much easier. Before computers, a thief seeking the secret to a competitor's product might have been required to break into a locked file cabinet and steal thousands of pages of blueprints. Today, all of that information may be available on computer networks—including shared networks—and may be contained on a storage device the size of a coin.[9] Changing employment patterns and social norms also contribute, as employees are increasingly mobile, and decreasingly loyal.[10]

And, although employees may pose the biggest security risk for trade secret owners,[11] they are not the only risk, as "organized criminals, including mafia-style organizations," become increasingly involved in cybercrime.[12] Finally, geopolitical changes have also contributed to the increase in trade secret theft. In 1992, then-CIA Director Robert Gates told Congress that:

> [W]hile the end of the Cold War did not bring an end to the foreign intelligence threat, it did change the nature of that threat. The threat has become more diversified and more complex. In a world that increasingly measures national power and national security in economic terms as well as military terms, many foreign intelligence services around the world

5. *See* The New Yorker (Mar. 1, 1952) ("We liked Willie Sutton's explanation of his chosen career. When asked why he robbed banks, Willie replied, 'I rob banks because that's where the money is.'").

6. United States v. Hsu, 155 F.3d 189, 194 (3d Cir. 1998) (citing Richard J. Heffernan & Dan T. Swartwood, Trends in Intellectual Property Loss 4, 15 (1996)).

7. S. Rep. No. 104-359 (1996), 1996 WL 497065 *8.

8. D. Alperovitch, *Revealed: Operation Shady RAT* (McAfee), *available at* http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

9. *See* David S. Almeling, *Seven Reasons Why Trade Secrets Are Increasingly Important*, 27 Berkeley Tech. L.J. 1091, 1098–99 (2012).

10. *Id.* at 1102.

11. Center for Responsible Enterprise and Trade (Create.org), *Trade Secret Theft: Managing the Growing Threat in Supply Chains* 11 (2012), *available at* https://create.org/resource/trade-secret-theft-managing-the-growing-threat-in-supply-chains/.

12. McAfee, Unsecured Economies: Protecting Vital Information 19, *available at* https://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf.

> are shifting the emphasis in targeting. Foreign targeting of American technology continues; technology is important for economic as well as military reasons. Since the U.S. continues to be on the cutting edge of technological innovation, technology theft will remain a major concern for us.[13]

In enacting the EEA, Congress said, it "use[d] the term economic or industrial espionage advisedly:"

> Espionage is typically an organized effort by one country's government to obtain the vital national security secrets of another country. Typically, espionage has focused on military secrets. But even as the cold war has drawn to a close, this classic form of espionage has evolved. Economic superiority is increasingly as important as military superiority. And the espionage industry is being retooled with this in mind.[14]

As information became more and more valuable as property, prosecutors found themselves required to "shoehorn economic espionage crimes into statutes directed at other offenses,"[15] with varying degrees of success. For example, the National Stolen Property Act (NSPA) by its terms requires proof that a defendant transported a physical object ("goods, wares, merchandise, securities or money") across state lines.[16] In 1985, the Supreme Court overturned a conviction under the NSPA based on the shipment of "bootleg" recordings of unlicensed trademarked performances.[17] The Court noted that the valuable property stolen was not the physical disks containing the recordings, but the protected performances, and that "the taking that occurs when an infringer arrogates the use of another's protected work" does not "comfortably fit[] the terms associated with physical removal employed by [the NSPA]."[18] A trade secret may be stolen without the carrying off of any physical object—for example, it may simply be memorized.

---

13. H. Rep. No. 359, 104th Cong. (1996), 1996 WL 497065 *7–8 (citing "The Threat of Foreign Economic Espionage to U.S. Corporations: Hearings Before the Subcomm. on Economic and Commercial Law of the House Comm. on the Judiciary," 102d Cong., 2d Sess. 59 (1977) (statement of Robert Gates, director of the Central Intelligence Agency).

14. H. Rep. No. 359, 104th Cong. (1996), 1996 WL 497065 *7; *but see* David S. Levine & Sharon K. Sandeen, *Here Come the Trade Secret Trolls*, 71 Wash. & Lee L. Rev. 230, 239 (2015) (the "dearth of reliable data" and "lack of understanding of trade secrecy's nuances" make it impossible to determine the extent of trade secret misappropriation via cybersecurity breaches"), *available at* http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1013&context=wlulr-online.

15. United States v. Hsu, 155 F.3d 189, 194 (3d Cir. 1998).

16. 18 U.S.C. § 2314.

17. Dowling v. United States, 473 U.S. 207 (1985).

18. *Id.* at 217.

Since the EEA was enacted two decades ago, it has steadily assumed a more important, and more visible, role as a law enforcement tool. In 1999, then-Deputy Attorney General Eric Holder stated that because intellectual property theft was "soaring," the Department of Justice had "concluded that we must make these types of crime a major law enforcement priority," and promulgated "the first, comprehensive inter-agency plan to combat the growing surge in the theft of intellectual property."[19] In 2013, Holder reported that between 2000 and 2010, DOJ had "secured well over 100 convictions in cases involving criminal trade secret thefts."[20]

This book is intended as a practical guide for practitioners as the investigation and prosecution of economic espionage and trade secret theft assume a more central place in the U.S. criminal justice system. Two decades of practice under the statute has yielded a body of case law which—although it will surely change and evolve as technology and the economy change and evolve—provide guideposts of the prosecutors, defense lawyers, and courts who will litigate and decide what is for sure to be an increasing number of cases under the statute.

Chapter 1 recounts the cultural, economic, and legal factors that led to passage of the EEA. Perceiving that changes in the economy had left "gaps" in federal and state law, Congress set out to provide, in the EEA, a "'comprehensive' mechanism for curtailing the escalating threat of corporate espionage."[21]

Chapter 2 describes the infrastructure the U.S. government has put in place over the past two decades to enforce the EEA and other criminal prohibitions against the theft of intellectual property. That infrastructure involves coordination between federal entities, including the White House, the Department of Justice, and the FBI, between federal and state governments, and between law enforcement agencies and private industry. Chapter 2 also addresses international cooperation between the U.S. and other nations in combating the theft of trade secrets.

Trade secrets are property rights, but because these rights are independent of any physical manifestation, law enforcement agencies often use specialized investigative means to investigate thefts, including undercover "sting" operations, computer searches, and electronic surveillance, including electronic surveillance

19. Remarks of Eric H. Holder, Jr., Deputy Attorney General, U.S. Department of Justice, July 23, 1999, *available at* https://web.archive.org/web/20000604154816/http:/www.cybercrime.gov/dagipini.htm.

20. U.S. Department of Justice, Attorney General Eric Holder Speaks at the Administration Trade Secret Strategy Rollout (Feb. 20, 2013), *available at* https://www.justice.gov/opa/speech/attorney-general-eric-holder-speaks-administration-trade-secret-strategy-rollout.

21. United States v. Hsu, 155 F.3d 189, 201 (3d Cir. 1998); United States v. Yang, 281 F. 3d 534, 543 (6th Cir. 2002) ("the purpose of the EEA was to provide a comprehensive tool for law enforcement personnel to use to fight theft of trade secrets").

under the Foreign Intelligence Surveillance Act. Chapter 3 addresses these investigative methods.

The EEA creates two separate offenses, one the theft of trade secrets for the benefit of a foreign government, and the other involving trade secret theft committed for private economic gain. The two offenses share a number of common elements, including the definitions of "trade secrets" and "misappropriation." Chapter 4 describes these common elements.

Chapter 5 enumerates the specific requirements of 18 U.S.C. 1831, which forbids "economic espionage," or the theft of trade secrets for the benefit of a "foreign government . . . instrumentality or . . . agency." The elements specific to this offense—including the connection to a foreign sovereign entity—are not required to prove a violation of 18 U.S.C. 1832, which penalizes "private" trade secret theft.

Chapter 6 describes the elements specific to section 1832, and that are not required under section 1831. These include a connection to interstate commerce, the necessary basis for federal jurisdiction.

Chapter 7 addresses a number of defenses to charges under the EEA. These include reverse engineering, which the law permits and indeed protects as an engine of technological progress. Chapter 7 also addresses the doctrine of "general skill and knowledge," which often comes into play when an employee leaving one company goes to work for a competitor, and requires courts to differentiate between the theft of information rightly belonging to the former employer, and the "general skill and knowledge" acquired by the employee in performing her job.

Chapter 8 describes the punishments applicable to those who violate the EEA. These can include imprisonment, forfeiture, and restitution orders.

Since the value of a trade secret lies in the fact of its secrecy, enforcement of the EEA—including the public filing of charges and a trial that may be widely reported—risks loss to the trade secret owner of precisely the property right the EEA is meant to protect. Chapter 9 describes the provisions made in the EEA to prevent that, including the use of protective orders and, where necessary, the closing of proceedings to the public.

Chapter 10 addresses the issue of successive prosecutions under the EEA. The EEA expressly states that it does not preempt state law, which can result in an individual being tried for the same theft in both federal and state court.

The threat of trade secret theft by foreign interests was clearly one of Congress's chief concerns in enacting the EEA,[22] and Chapter 11 details the unique issues

22. For example, Robert Gates, then director of the CIA, told Congress:

> Our fundamental assessment is that while the end of the Cold War did not bring an end to the foreign intelligence threat, it did change the nature of that threat. The threat has

raised by international enforcement of the statute. These include the extraterritorial application of U.S. law, obtaining jurisdiction over foreign defendants, and diplomatic issues raised when a trade secret is alleged to have been stolen for the benefit of a foreign government.

Finally, in 2016, Congress amended the EEA to provide for a private civil cause of action, allowing the owners of misappropriated trade secrets to seek damages in federal court. In addition, the law authorizes equitable relief and the award of attorneys' fees in certain circumstances. And it provides aggrieved trade secret owners with a powerful weapon, authorizing courts, "upon ex parte application but only in extraordinary circumstances," to order the "seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action."[23] Chapter 12 analyzes the new provision.

become more diversified and more complex. In a world that increasingly measures national power and national security in economic terms as well as military terms, many foreign intelligence services around the world are shifting the emphasis in targeting. Foreign targeting of American technology continues; technology is important for economic as well as military reasons. Since the U.S. continues to be on the cutting edge of technological innovation, technology theft will remain a major concern for us.

S. Rep. No. 104-359 (1996), 1996 WL 497065 *7 (citing "The Threat of Foreign Economic Espionage to U.S. Corporations: Hearings Before the Subcomm. on Economic and Commercial Law of the House Comm. on the Judiciary," 102d Cong., 2d Sess. 59 (1977) (statement of Robert Gates, director of the Central Intelligence Agency).

23. 18 U.S.C. § 1836(b)(2)(A)(i).