CHAPTER ONE

Dimensions of Economic Espionage and the Criminalization of Trade Secret Theft

WE LIVE in a world in which the economic health of nations and the competitiveness of businesses are determined largely by the ability to develop, commercialize, and capture the economic benefits from scientific and technological innovations. As the Internet and technological advances continue to reshape the way we do business in government and industry, and as competition and economic pressures create quicker and more efficient ways to do business, the reality of increased economic crimes has a serious impact. The connectivity of the Internet has made the concept of borders and jurisdictions an incredible challenge in combating this problem. Organized groups of criminals can easily commit economic crimes and avoid sanctions across what were once clearly defined jurisdictions, necessitating increased cooperation among the global criminal justice agencies. A greater understanding of how technology, competition, regulation, legislation, and globalization interact is needed to successfully manage the competition between economic progress and criminal opportunity.

The reach of criminal sanctions has expanded in the realm of technology. The revolution in information technologies has changed society fundamentally and will continue to do so in the foreseeable future. The development of information technology has given rise to unprecedented economic and social changes, which also have a dark side. The new technologies challenge existing legal concepts. Information and communications flow more easily around the world. Borders are no longer boundaries to this flow. Criminals are increasingly located in places other than where their actions produce their effects.

Today's information age requires businesses to compete on a worldwide basis, sharing sensitive information with appropriate parties while protecting that information against competitors, vandals, suppliers, customers, and foreign governments. Lawmakers are increasingly resorting to criminal codes

to establish economic and social policies regarding the use and dissemination of technology. Many fear that technological advances are making corporate spying and theft of "intellectual capital" both easier and cheaper. In the global economy, there is less distinction between the need to protect the interests of the state and the need to protect commercial interests. A nation's economic status makes up a large part of its national security. This economic status is dependent on a nation's ability to compete effectively in the world market.

Intellectual property crimes are serious crimes in their own right, not because they inflict physical injury or death upon a person, but rather because they steal a creative work from its owner. Intellectual property theft is rampant, but largely silent, so corporations and law enforcement alike have trouble grasping its enormous impact on profitability – not to mention on national economies. Although civil remedies may provide compensation to wronged intellectual property rights holders, criminal sanctions are often warranted to ensure sufficient punishment and deterrence of wrongful activity. Indeed, because violations of intellectual property rights often involve no loss of tangible assets and, for infringement crimes, do not even require any direct contact with the rights holder, the rights holder often does not know it is a victim until a defendant's activities are specifically identified and investigated.

In the United States, Congress has continually expanded and strengthened criminal laws for violations of intellectual property rights specifically to ensure that those violations are not merely a cost of doing business for defendants. However, domestic laws are generally confined to a specific territory. Thus, solutions to the problems posed must be addressed by international law and international cooperation, necessitating the adoption of adequate international legal procedures. Law enforcement officials in the United States, apparently viewing the U.S. economy as the most likely target, have begun to focus on this new form of crime and the U.S. Congress has handed them a new enforcement tool in the Economic Espionage Act (EEA). This law, although relatively new, has far-ranging international implications. It is a trap for unwary foreign competitors who compete aggressively with U.S.-based companies. It also may serve as a model that will be followed by other nations with similar legislative or law enforcement initiatives. In those countries where the government plays a role in encouraging industrial activity, the conflict between economic nationalism and international competition will be an ongoing problem. It remains to be seen whether U.S. initiatives in this area are the start of an international trend or whether the United States will stand alone.

The most obvious legislative deficiency with which law enforcement has to deal is the absence of comprehensive legislation relating to offenses committed in an electronic environment. Some countries have none at all,

some have adopted measures that have been integrated awkwardly into existing legislation, but relatively few have adequately updated their penal codes. Even after legislation is introduced at the national level, many problems will remain unless governments at the same time address the transnational nature of high-tech crime, which may originate in one country and have consequences in a second, while the evidence may be spread through many more. At present, there are no guidelines concerning which country's laws should prevail in pursuing an offense, how court decisions can be enforced if defendants reside abroad, and which protocols govern cross-border investigations.

Criminal Consequences of Trade Secret Theft

The American people have had contradictory views of economic crimes for some time, seeing these crimes as either a minor issue or a major crisis. Since the mid-1980s, there have been times when they have been in the limelight because of a financial crisis (e.g., the savings and loan scandal and the insider trading problems in the 1980s). Usually, they have taken a backseat to a strong national focus on more conventional crimes, specifically violent crimes.

For example, even a cursory evaluation of internal corporate security operations and protection procedures demonstrates that U.S. corporations view the issue of security as one of protecting people and tangible, physical assets rather than intellectual property. Given such a traditional approach to security, this particular attitude is not readily adaptable to providing protection against economic espionage. Many companies do not even recognize the significant loss that is suffered when trade secrets are pilfered by foreign intelligence services; they may simply view it as a process that is going to occur regardless of what they do.

Economic espionage and trade secret theft are considered white-collar offenses. The phrase *white-collar crime* was coined in 1939 during a speech given by Edwin Sutherland to the American Sociological Society. Sutherland defined the term as "crime committed by a person of respectability and high social status in the course of his occupation." Although there has been some debate as to what qualifies as a white-collar crime, the term today generally encompasses a variety of nonviolent crimes usually committed in commercial situations for financial gain. Many white-collar crimes are especially difficult to prosecute because the perpetrators are sophisticated criminals who have attempted to conceal their activities through a series of complex transactions. According to the Federal Bureau of Investigation (FBI), white-collar crime is estimated to cost the United States more than $300 billion annually. However, the protection of trade secrets is considered to be increasingly important to the competitiveness of the world's industrial sector.

At the same time, the world has been undergoing a computer revolution. Since at least the beginning of the 1990s, the power of information technology has grown exponentially, resulting in increasingly powerful means for the theft and transfer of protected information. This technological evolution in open societies facilitates the emergence of certain kinds of criminal and subversive activities, such as economic espionage. Thus, security (both economic and physical) in light of the recent evolution in technology and changes in geopolitical tensions is the broader topic surrounding this book.

The central focus of this book revolves around the following questions: Should the taking of information be criminalized as it has been, for example, in the United States by the EEA? Does the prospect of the threat of prosecution serve as a true deterrent for corporate espionage under the EEA? How can economic espionage be made less appealing? Which would be more effective, prosecution or heavier fines? For example, should violator companies be sanctioned internationally, whereby they cannot reap any benefits from the stolen information? Are criminal laws in this area indispensable to competitiveness? Is it unnecessary? Or is it perhaps even counterproductive? The book's focus on economic espionage reflects an underlying belief in the importance of industrial policy as a topic in the broader context of national and international security concerns.

Furthermore, the lack of agreed-upon definitions regarding economic and high-tech crimes has resulted in a paucity of data and information on the size and scope of the problem. There are no national mechanisms, such as the *Uniform Crime Reports*, for the reporting of economic crimes by law enforcement. Academics have not been able to agree on definitions and have, for the most part, continued to focus on white-collar crime. However, although most social scientists acknowledge that economic espionage is a major problem, especially in the digital age, the topic remains underrepresented in the social science literature, including criminological and sociological literature.

This book brings together a wide variety of materials that deal with the frequently neglected criminological dimension of economic espionage. The book's purpose is twofold: first, to present an assessment of the state of economic espionage activities within a criminological context and, second, based on that assessment, to address areas where additional research, legislative action, training, cooperation between law enforcement and the private sector, and international cooperation are required.

The data presented in this book are a result of years of interaction with practitioners, industry representatives, and government officials prosecuting and investigating these types of crimes. The data presented provide the basis for a discussion to address the topic of economic espionage, both as a crime and as a national security issue. It points out the challenges that lie ahead in today's contemporary global economy for the law enforcement

community, policy makers, and legislators. There is a need for a critical discussion about the definition of this problem, the source of the problem, and the purpose behind the enactment of the EEA legislation. The material presented here is intended to encourage a dialogue about what is meant by criminalization of intellectual property crimes, such as information theft and trade secret theft, whether information should be considered "property," and the role of law enforcement in policing economic espionage activities. Beyond these concerns, the book draws attention to a variety of issues raised by economic espionage and technological development. Many of these problems are derived from an environment in which there is little face-to-face interaction and identification of the perpetrator is difficult to establish. It is not only the environment that poses problems for law enforcement but also the technology itself. The discussions address the need for the education and training of law enforcement personnel who deal with these problems. Such educational initiatives should be extended to effect change in the attitudes of the judiciary and the wider public concerning prevention of information theft and technology crimes.

Economic espionage is not merely an intelligence issue; it involves fundamental questions about a nation's economic interests, which in turn are part of its national security. For example, the arrest of the senior FBI official Robert Hanssen in February 2001 reminded America of the dangers of foreign spying against U.S. national security interests.[1] As the legislative history to the EEA stated: "typically, espionage has focused on military secrets. But as the Cold War came to an end, this classic form of espionage evolved. Nations around the world recognize that economic superiority is increasingly as important as military superiority."

Theoretical Perspectives

One philosophical rational for regarding knowledge as property is the labor reward theory, a theory that finds foundation in the work of John Locke.[2] Locke, in his famous *Two Treatises of Government*, stated: "Whatsoever then he removes out of the State that Nature hath provided, and left it in, he hath mixed his Labor with, and joined to it something that is his own, and thereby makes it his Property."[3] This reasoning applies to the creation of new scientific knowledge.

Two prominent and competing theories, retribution and utilitarianism, might justify the punishment of information thieves as criminals. Both retributive and utilitarian arguments are useful in understanding the conflict that seems to have arisen between two sets of social values: those who seek to protect private rights by means of the criminal justice system and those that argue that society benefits more with the basic principles of freedom from interference, freedom of information, freedom of expression, and

the like. The question then becomes whether either traditional retributive or utilitarian theory provides a justification for the imposition of criminal punishment.

Proponents of retribution argue that, regardless of the effects of punishment, society is always justified in imposing criminal sanctions on those who violate the moral order. All retributive arguments in favor of punishment assume that we can define the moral order we seek to protect. In light of utilitarian theories of punishment, the question becomes what kind of behavior do we want to deter and what kind of behavior do we want to encourage to arrive at utilitarian gain?

In a civil suit, the issue before the court is usually how much harm the plaintiff has suffered at the hands of the defendant and what remedies, if any, are appropriate to compensate the victim for his or her loss. The goal of civil litigation is compensation. By contrast, a criminal case requires the court to determine whether and to what extent the defendant has injured society. The result of criminal conviction is a sentence designed to punish. Criminal law seeks to punish because society recognizes that we cannot adequately respond to certain courses of action merely by rendering compensation to the victim.

Legal theories about the justification for punishment can be grouped into two main categories: retributionism and utilitarianism. Retribution is an ancient concept. Opponents of the theory have argued that it is an outmoded, even barbaric, idea, inappropriate in an enlightened society.[4] The classic, modern statement of the concept of retributive justice is found in Kant's *The Philosophy of Law*:

> Juridical punishment can never be administered merely as a means of promoting another good, either with regard to the Criminal himself or to Civil Society, but must in all cases be imposed only because the individual on whom it is inflicted has committed a Crime. . . . The Penal Law is a Categorical Imperative; and woe to him who creeps through the serpent-windings of Utilitarianism to discover some advantage that may discharge him from the Justice of punishment, or even from the due measure of it, according to the Pharisaic maxim: "It is better that one man should die than that the whole people should perish." For if Justice and Righteousness perish, human life would no longer have any value in the world.[5]

Most utilitarian arguments on the value of punishment can be categorized as a theory of deterrence, restraint, or reformation. According to Jeremy Bentham, punishment serves the purpose of deterring socially undesirable behavior due to a "spirit of calculation" we all possess:

> Pain and pleasure are the great springs of human action. When a man perceives or supposes pain to be the consequence of an act, he is acted upon in such a manner as tends . . . to withdraw him . . . from the commission of that

> act. If the apparent magnitude, or rather, value of that pain be greater than the apparent magnitude or value of the pleasure or good he expects to be the consequence of the act, he will be absolutely prevented from performing it.[6]

Jeremy Bentham formulated the principle of utility as part of such a theory in *Introduction to the Principles of Morals and Legislation* in 1789. An action conforms to the principle of utility if and only if its performance will be more productive of pleasure or happiness, or more preventive of pain or unhappiness, than any alternative. Instead of "pleasure" and "happiness" the word "welfare" is also apt: The value of the consequences of an action is determined solely by the welfare of individuals.

A characteristic feature of Bentham's theory is the idea that the rightness of an action *entirely* depends on the value of its consequences. This is why the theory is also described as consequentialist. Bentham's theory differs from certain other varieties of utilitarianism (or consequentialism) by its distinctive assumption that the standard of value is pleasure and the absence of pain, by being an act-utilitarian, and by its maximizing assumption that an action is not right unless it tends toward the optimal outcome.

These theories provide useful tools for examining the topics of this book. They are reexamined in connection with some of the conclusions in the final chapter, where policy choices are analyzed. These theories provide justification for the move toward criminalization of certain intellectual property theft.

Spies Target Our Know-How

Trade secret theft, or economic espionage as it is often called, commonly occurs in one of two ways: (1) a disgruntled employee misappropriates the company's trade secrets for his or her own financial benefit or to harm the company or (2) a competitor of the company or a foreign nation misappropriates the trade secret to advance its own financial interests.[7] The manner in which these thefts occur ranges from the complex (computer hacking, wire interception, spy devices) to the mundane (memorization, theft of documents, photocopying).

There are many varieties of spies. Some of the more common international snoops include competitors, vendors, investigators, business intelligence consultants, the press, labor negotiators, and government agencies.[8] Espionage employees are often talented people with highly analytical skills who excel at quickly collecting and synthesizing significant quantities of information.[9] Some countries hire individuals, rather than large organizations or intelligence agencies, to do their spying for them.[10] Other countries hire teams of individuals to enter foreign companies and steal ideas. The tools of the espionage community include scanning trade-show floors,[11]

combing through web sites,[12] reviewing filings with regulatory agencies,[13] eavesdropping in airline terminals and on airline flights,[14] taking photographs of factories and business offices,[15] using data-mining software to search the Internet at high speeds for information,[16] using "shadow teams,"[17] stealing laptop computers,[18] tuning in to computer monitors from a nearby location using surveillance equipment,[19] attending competitors' court trials,[20] and even "dumpster diving."[21] However, in all instances, the owner – who often has invested hours of hard work and millions of dollars in developing the trade secret – is deprived of the commercial advantage he or she would have obtained by keeping the trade secret unavailable to his or her competitors and the public.

Economic Espionage Becoming Big Business

A number of factors have contributed to the increase in trade secret theft in recent years, such as the end of the Cold War, increased access to and use of computer technology, greater profitability, and the lack of company resources to investigate and pursue such theft.[22] The increasing importance of economic factors in defining a nation's security has resulted in the widespread theft of proprietary information in the form of trade secrets. The level of trade secret theft appears to have skyrocketed in recent years, and it includes more capers than the celebrated Amazon.com–Wal-Mart employee poaching case,[23] the improper use of the Sabre computer system by an American Airlines employee,[24] and the Oracle–Microsoft "dumpster diving" case.[25] Realistically, no business is immune from economic espionage. Targets include two main forms: industry and proprietary business information.[26] Government and corporate financial and trade data are also stolen on a regular basis.

The United States leads the world in developing new products and new technologies.[27] Per capita, the United States produces the majority of the world's intellectual property capital, including patented inventions, copyrighted material, and proprietary information.[28] Within the United States, economic espionage occurs with the greatest frequency in regions with high concentrations of technology and research and development activities. The FBI has reported that at least twenty-three foreign governments actively target the intellectual property of U.S. corporations.[29] Another FBI study also found that of 173 countries, 100 were spending resources to acquire U.S. technology.[30] Of those 100 countries, 57 were engaging in covert operations against U.S. corporations.[31] According to the FBI study, the following countries allegedly are extensively engaged in espionage activities against American companies: France, Israel, Russia, China, Iran, Cuba, the Netherlands, Belgium, Germany, Japan, Canada, India, and several Scandinavian countries.[32] Examples of the most targeted regions for spying include Silicon

Valley, Detroit, North Carolina, Dallas, Boston, Washington, DC,[33] and the Pennsylvania–New Jersey area,[34] where many pharmaceutical and biotechnology companies are headquartered.[35] Silicon Valley, according to some experts, is the most targeted area. It offers an ideal setting for economic espionage because of its concentration of electronics, aerospace, and biotechnology industries; its national ties to the Far East; and its mobile, multinational workforce. In Silicon Valley alone, more than twenty FBI agents are assigned full time to investigations of trade secret theft. In particular, high-tech businesses, pharmaceutical companies, manufacturing firms, and service industries are the most frequent targets of corporate spies.[36] The most frequently targeted industries appear to include aerospace, biotechnology, computer software and hardware, transportation and engine technology, defense technology, telecommunications, energy research, advanced materials and coatings, stealth technologies, lasers, manufacturing processes, and semiconductors.[37] Victims are not just the naïve and unsophisticated – they include such corporate giants as General Motors, Intel, Lockheed Martin, and Hughes Aircraft.[38] Further, it is not just "high-technology" information that is a target. Proprietary and confidential business information such as customer lists and information, product development data, pricing data, sales figures, marketing plans, personnel data, bid information, manufacturing costs analyses, and strategic planning information are also sought out by intelligence agents.[39] Japan, Taiwan, South Korea, China, the former Soviet Union, and the Russian Republic have devoted the most resources to stealing Silicon Valley technology.[40] Nearly every major U.S. company now has a competitive intelligence office that is designed to discover the trade secrets of competitors.[41] Some firms, such as Motorola, have intelligence units located around the world.[42]

Computers Spark Surge in Trade Secret Theft

No single reason can be given for the increase in trade secret theft. However, one reason for the dramatic increase is undoubtedly the world's ever-expanding use of the computer. Increasing public use and access to computers has allowed people who harbor criminal intentions to copy sensitive information or to enter confidential areas to which they previously had no access. For example, a disgruntled employee who wants to take the company's most attractive new plan or product to his or her next employer no longer needs to spend hours clandestinely duplicating documents. He or she can now download the plans, schematics, or documents to a 3.5-in. computer disk in a matter of seconds.[43] Every time a new computer is linked to a network, or a company network is linked to the Internet, the points of entry through which a hacker may gain access to a company's confidential system are increased. Each new addition increases the chance that someone

will not follow the proper security instructions or will allow access to an unauthorized user.[44]

Not only has confidential and proprietary business information become easier to steal, but stealing it is also potentially very lucrative.[45] For example, a group of Russian computer hackers stole $10 million from Citibank by infiltrating its computer network.[46] One businessman has stated: "if I want to steal money, a computer is a much better tool than a handgun . . . it would take me a long time to get $10 million with a handgun."[47]

Proprietary Information

Generally, such information concerns business and economic resources, activities, research and development, policies, and critical technologies. Although it may be unclassified, the loss of this information could impede the ability of a nation to compete in the world marketplace and could have an adverse effect on its economy, eventually weakening its national security. Commonly referred to as "trade secrets," this information typically is protected under both state and federal laws in the United States. A misappropriation of trade secrets, or industrial espionage, occurs when a trade secret is obtained by a breach of a confidential relationship or through improper means, when such information is used, and when such use causes the trade secret owner to sustain damages.

Global Competition and Intellectual Property Rights

Economic espionage especially threatens intellectual property rights (IPRs), which have become the most valuable asset of global business.[48] IPRs can be owned or stolen for profit and are a vital issue in today's competitive market economy. IPRs have become an area of international interest and controversy as the rate and cost of technological progress have increased and as national borders have become ever more transparent. Intellectual property refers to the legal rights that correspond to intellectual activity in the industrial, scientific, and artistic fields.[49] These legal rights, most commonly in the form of patents, trademarks, and copyright, protect the moral and economic rights of the creators, in addition to the creativity and dissemination of their work.[50] Industrial property,[51] which is part of intellectual property, extends protection to inventions and industrial designs.

The costs of product development in the innovation and expression industries are high. For example, filmmaking, music producing, and research-oriented pharmaceuticals manufacturing are risky businesses that survive with three successes out of ten tries. In contrast, the costs of product imitation (or outright theft) are relatively low. The theft in question is not,