

Spring 1999

Corporate and Economic Espionage: A Model Penal Approach for Legal Deterrence to Theft of Corporate Trade Secrets and Propriety Business Information

Christopher A. Ruhl

Follow this and additional works at: <https://scholar.valpo.edu/vulr>



Part of the [Law Commons](#)

Recommended Citation

Christopher A. Ruhl, *Corporate and Economic Espionage: A Model Penal Approach for Legal Deterrence to Theft of Corporate Trade Secrets and Propriety Business Information*, 33 Val. U. L. Rev. 763 (1999).

Available at: <https://scholar.valpo.edu/vulr/vol33/iss2/8>

This Notes is brought to you for free and open access by the Valparaiso University Law School at ValpoScholar. It has been accepted for inclusion in Valparaiso University Law Review by an authorized administrator of ValpoScholar. For more information, please contact a ValpoScholar staff member at scholar@valpo.edu.



Ruhl: Corporate and Economic Espionage: A Model Penal Approach for Lega

CORPORATE AND ECONOMIC ESPIONAGE: A MODEL PENAL APPROACH FOR LEGAL DETERRENCE TO THEFT OF CORPORATE TRADE SECRETS AND PROPRIETARY BUSINESS INFORMATION

I. INTRODUCTION

Crime knows few limits when greed is at stake and technology is a weapon.¹ Intel, the computer chip maker has revolutionized the computer industry through the invention of a single product, the Pentium processor.² Intel developed the current Pentium processor through years of research, development and modification.³ However, through the unscrupulous acts of one person, the company's competitors could have obtained the information necessary to produce an identical product for a fraction of the cost, effort and time, threatening to put Intel out of business.⁴ Recently, an employee at Intel decided to steal the blueprints for the Pentium processor.⁵ The employee attempted to download the files to a remote site, his home computer.⁶ While the computer files could be viewed remotely by authorized people, Intel's internal computer system would not allow these critical files to be

¹ Jeffrey Young, *Spies Like Us*, FORBES, June 3, 1996, at 70.

² Of the 83 million computer machines sold during 1997, the Intel chip powered over ninety percent. Joshua Cooper Ramo, *A Survivor's Tale*, TIME, Dec. 29, 1997, at 54. Ramo characterizes Intel as a "super efficient firm with monopoly like returns gliding past competitors and, not incidentally, racking up huge profits". *Id.* at 58. For the fiscal year 1996, Intel produced revenue totaling \$ 26 billion and recorded profits of \$ 6 billion. 1998 *Intel Annual Report* (visited Apr. 19, 1999) <<http://www.intel.com/intel/annual98/summary.htm>>. Both figures represent record marks for Intel. *Id.* The company attributes these records to "rapid market acceptance of the Pentium processor and the Pentium processor with MMX technology, both of which were introduced in 1997." *Id.*

³ A conservative survey estimates that Intel expended sums of money in the range of several hundred million dollars and years of exploration to develop cutting edge technology which eventually produced a product that could be marketed and sold in mass quantities. Pete Carey, *Software Engineer Charged in Theft of Pentium Plans from Intel*, THE SEATTLE TIMES, Sept. 24, 1995, at A8. According to 1997 data, Intel spends approximately \$2.67 billion on research and development annually. 1998 *Intel Annual Report* (visited Apr. 19, 1999) <<http://www.intel.com/intel/annual98/summary.htm>>. This represents 10 percent of total sales and accounts for one of Intel's largest single expenses. *Id.*

⁴ Michelle Cole, *Proliferation of High Tech Firms Fosters Espionage*, IDAHO STATESMAN, April 28, 1997, at 10B.

⁵ Cole, *supra* note 4, at 10B.

⁶ *Id.*

downloaded.⁷ However, this safeguard failed to deter the industrious thief.⁸ Rather than giving up, the employee displayed the files on the computer and proceeded to videotape each screen.⁹ With the information stored on tape, the employee possessed the information necessary to exactly duplicate the company's flagship product while only spending minimal amounts of money, time and effort.¹⁰ While the employee was arrested prior to transmitting this information to any third party, this narrative illustrates the rapidly growing problem of economic, corporate and industrial espionage upon the welfare of U.S. corporations.¹¹

As the example illustrates, "economic espionage is hardly a novel practice."¹² Currently, the Federal Bureau of Investigation (FBI) has approximately 800 probes pending involving theft of corporate trade

⁷ *Id.*

⁸ *Id.*

⁹ *Id.*

¹⁰ *Id.* Intel valued the information recorded in the theft in the "'tens of millions of dollars'". Carey, *supra* note 3, at A8. However, this figure does not account for the potential loss to sales, profits, competitive advantage, and market share. *Id.*

¹¹ The employee was eventually sentenced to 33 months in prison after pleading guilty to violating both the federal mail fraud and interstate transportation of stolen property statutes. Cole, *supra* note 4. See *infra* notes 52-84 for a discussion of both federal statutes. See also Ben Winton, *Intel Theft a Frame-Up?*, ARIZ. REPUBLIC, Sept. 26, 1995, at A1; *Man Charged in Theft of Trade Secrets*, DES MOINES REG., Sept. 26, 1995, at 8; *FBI Arrests Man in Theft of Secrets of Pentium*, SAN DIEGO UNION-TRIB., Sept. 25, 1995, at A3; *Engineer Who Stole Pentium Chip Secret Gets Prison Term*, SAN FRANCISCO CHRON., June 25, 1996, at A14. See also *infra* notes 13-19 and accompanying text discussing the rising problem of theft of confidential business information.

¹² Stan Crock, *Business Spies: The New Enemy Within?*, BUS. WK., February 10, 1997, at 16. "The ground rules have changed, and the battlefield is now economic rather than ideological, but espionage in the 1990's springs directly from the ruins of the Cold War spy regimes." JOHN F. FIALKA, *WAR BY OTHER MEANS: ECONOMIC ESPIONAGE IN AMERICA* (1997) (jacket cover). In a bitterly contested lawsuit still pending, Dow Chemical won a restraining order to prevent General Electric (GE) from exploiting trade secrets regarding the plastic casing surrounding a car's instrument panel invented and manufactured by Dow Chemical. Richard Waters, *Not Spying, Just Hiring*, FIN. TIMES, Apr. 3, 1997 at 7. Dow Chemical alleged that GE had made a calculated play to gain knowledge of Dow's manufacturing process, design, and marketing initiatives by hiring 14 employees from Dow's plastics division and placing the workers in similar jobs where they would inevitably use their former employer's trade secrets. *Id.* at 8. Disputes like this and the controversy between General Motors (GM) and Volkswagen in the early 1990s demonstrate the widespread problem of what is generally termed industrial, economic, or corporate espionage. For a detailed discussion of the GM and Volkswagen dispute, see Richard J. Reibstein, *Protecting Secrets and Personnel from the 'Lopez Effect'*, N.Y. L.J., Dec. 17, 1996, at 1.

secrets by foreign countries alone.¹³ For 1997, estimates measure the economic loss to U.S. corporations at over three hundred billion dollars.¹⁴ The importance of protecting intellectual property rights of U.S. corporations is paramount in today's technologically based economy.¹⁵

¹³ Ronald E. Yates, *Corporate Cloak and Dagger*, CHI. TRIB., Sep. 1, 1996, at B1. This translates to a 100% increase in the FBI caseload over the previous year. *Id.* Furthermore, a survey released in 1996 indicates a 323% increase in reported incidents over the four-year period from 1992-1995. Crock, *supra* note 12, at 16. More importantly, recent investigations have discovered over 23 foreign countries are directly engaging in covert espionage activity, while over 100 foreign countries have spent public funds to help companies obtain American technology and corporate trade secrets. Yates, *supra* note 13, at B1. France, Germany, Israel, China, Russia and South Korea were named as major offenders. Jack Nelson, *Spies Took \$300 Billion Toll on U.S. Firms in '97: FBI Says Espionage is Increasing, With at Least 23 Governments Targeting American Companies*, LOS ANGELES TIMES, January 12, 1998, at A1. Nelson reports that over 1,100 documented incidents of economic espionage were reported to the FBI by major companies last year. *Id.*

¹⁴ Nelson, *supra* note 13, at A1. Nelson reports this figure as representing the first national survey undertaken by the FBI and its agent Edwin Fraumann to quantify the intellectual property losses from both foreign and domestic espionage on U.S. based companies. *Id.* Other estimates quantify the economic loss from 20 billion up to 100 billion dollars annually. Yates, *supra* note 13, at B1. A compounding problem with accurately measuring the actual impact on the U.S. economy is the failure of corporations to detect and to report theft of trade secrets and proprietary information. Yates, *supra* note 13, at B1. An FBI spokesman explained, "You never hear about successful economic espionage cases. They can go on for years without anybody knowing it." *Id.* See also IRA S. WINKLER, CORPORATE ESPIONAGE 166-70 (1997) (Some companies' security systems may be so lax that a company is simply unaware that information has been stolen). Thousands of cases escape detection each year and thousands of cases are detected and never reported by corporations. *Id.* The practical reasons corporations may decline to pursue an action result from the fear that publicity will directly impair their stock value, customer confidence, and business competitiveness. See generally Michael A. Epstein & Stuart D. Levi, *Protecting Trade Secret Information: A Plan for Proactive Strategy*, 43 BUS. LAW. 887 (1988); R. EELS & P. NEHEMKIS, CORPORATE INTELLIGENCE AND ESPIONAGE 118 (1984) (Most executives would rather bury the losses in earning statements than admit they have lost the family jewels). However, I will argue the main reason for reluctance to report economic espionage is the lack of effective laws to adequately punish and deter such activity. This is the basis for the thesis of this Note and for developing a model penal statute. See *infra* Sections II, III, IV.

¹⁵ As Senator Rockefeller advised,

Intellectual property is the seed corn that builds our national income, our social well-being, and our national competitiveness. When the intellectual property of Americans is not protected, our country loses not only jobs, production and profits today, but also our ability to undertake the research and the investments that lead to further technological progress tomorrow.

Peter J. G. Toren, *The Prosecution of Trade Secrets Thefts Under Federal Law*, 22 PEPP. L. REV. 59, 60 n.5 (1994). See also JOHN F. FIALKA, WAR BY OTHER MEANS: ECONOMIC ESPIONAGE IN AMERICA (1997). "[T]he secret operations of America's enemies (and friends) threaten to

Corporate trade secrets and proprietary information represent the most valuable economic and business resource for gaining competitive advantage and market share in the U.S. free market economy.¹⁶ The U.S. economy depends on increased efficiency, productivity and technological advancement gained through the development and implementation of new processes, products and services.¹⁷ However, this global economic environment fosters a powerful incentive for corporations, individuals and foreign governments to use improper and illegal means to gain the competitive advantage and market share necessary to survive and prosper.¹⁸ Furthermore, as technology

hollow out the U.S. economy and siphon away the jobs and technologies we need to remain competitive in the twenty-first century." *Id.* at book jacket cover. Louis Freeh, the acting director of the FBI, related the significance of economic espionage while testifying before the Senate Select Committee on Intelligence, stating "The theft, misappropriation, and wrongful receipt, transfer, and use of United States proprietary economic information...directly imperils the health and competitiveness of our economy." *Hearing on Economic Espionage Before the Senate Select Committee on Intelligence and Senate Committee on the Judiciary*, 104th Cong. 1718 (1996) (statement of Louis Freeh, Director, Federal Bureau of Investigation). As described by the Honorable Richard Posner, "The future of the nation depends in no small part on the efficiency of industry, and the efficiency of industry depends on the protection of intellectual property." *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 180 (7th Cir. 1991).

¹⁶ Information is the currency of competition. Epstein & Levi, *supra* note 14, at 887. A company's ability to be successful depends on its ability to acquire and maintain business information. *Id.* at 889. Moreover, gathering this information is time consuming and expensive. Don Weisner & Anita Cava, *Stealing Trade Secrets Ethically*, 47 MD. L. REV. 1076, (1988). Also, through technology and deregulation, a competitor can take the lead in an industry with a single innovation. Crock, *supra* note 12, at 17. Without valuable proprietary information and trade secrets, today's archrival may not be on the playing field tomorrow. The significance and importance of corporate trade secrets and proprietary business information cannot be understated in today's global economy. Louis Freeh, director of the FBI explained, "The development and production of proprietary economic information is an integral part of virtually every aspect of United States trade, commerce, and business and hence, is essential to maintaining the health and competitiveness of critical segments of the United States economy." *Hearing on Economic Espionage Before the Senate Select Committee On Intelligence And Senate Committee On The Judiciary*, 104th. Cong. 1718 (1996) (statement of Louis Freeh, Director, Federal Bureau of Investigation). President Clinton recently stated, "Trade secrets are an integral part of virtually every sector of our economy and are essential to maintaining the health and competitiveness of critical industries operating in the United States." *President Signs Economic Espionage Act*, J. OF PROPRIETARY RTS., Oct. 1996, at 15, 23. See also *supra* note 15 and accompanying text.

¹⁷ Epstein and Levi, *supra* note 14, at 890.

¹⁸ Why steal? This is somewhat self explanatory upon an understanding of the value of business information. See *supra* notes 15-16. Two factors also contribute to the mechanics of why companies steal proprietary information. First, obtaining and exploiting other people's work rather than creating and developing information from scratch is more simple, easy, and cost effective. See *infra* note 19. Widespread employee mobility and the sophisticated surveillance methods explain this theory. See *infra* note 19. Second, the

advances, the methods for stealing corporate trade secrets and proprietary information are becoming highly sophisticated, less expensive and easier to implement.¹⁹ Therefore, U.S. criminal law must

general business environment where earnings, profits, and stock price dictate whether a company is a success or failure provides a powerful motivation to cut corners and employ any means necessary to quickly bring new products and services to market in order to grow revenues and profits (or implementing a new process or strategy to reduce costs). See *supra* notes 1-10 and accompanying text. A representative example comes from Massachusetts. Charles Sennott, *Shadowy World of Spying*, ROCKY MTN. NEWS, Feb. 2, 1997, at 2F. FBI agents set up a sting after a theft of genetically altered cells occurred at a subsidiary of Genzyme. *Id.* Documents stated that with the stolen cells and a one million dollar investment the company receiving this information could produce a product that would otherwise cost over two hundred million dollars to develop. *Id.* As illustrated by this example, rather than expending years of time and huge sums of money to develop a competing product, the competitors realized that simply copying a proven formula would be easier, less expensive, and less risky. *Id.* The real fraud, as the example points out, was an attempt to bypass costly research and development and gain access to a potential market of two billion dollars through illegal theft. *Id.* The problem lies not in fostering competition among firms which produces a wider variety of products at a higher level of quality and lower price. The problem lies in the fact that stealing and misappropriating provides a disincentive to develop new technologies and processes. Rather than investing in research and development, it is easier and less expensive to pirate other corporation's business information. As Ben Venzke, publisher of the Washington-based Intelligence Watch Report, explains, "the underlying philosophy is why spend ten years and one billion dollars on research and development when you can bribe a competitor's engineer for one million dollars and get the same, if not better, results." *Id.* The bottom line is "Companies are willing to do anything and go anywhere to get a competitive edge." Jeff Louderback, *Paper Chase: Every Business is Susceptible to Theft and Espionage and the Danger Lurks in the Places You'd Least Expect*, DAYTON SMALL BUS. NEWS, Aug. 1, 1996, at 6.

¹⁹ Virtually every sophisticated espionage tactic used during the Cold War is being used today against American companies. Yates, *supra* note 13, at B1. Methods for stealing valuable corporate information include dumpster diving (rummaging through corporate trash receptacles), data dipping (hacking into computer databases, allowing data to be viewed and duplicated through remote computer modem access) and inserting electronic eavesdropping equipment such as phone taps, wireless microphones, and mini-cameras placed strategically in air ducts, office walls, and baseboard heaters. *Id.* See also Nelson, *supra* note 13, at A1 (intrusive methods include eavesdropping by wiretapping and bugging offices, bribing suppliers and employees, planting "moles" in a company, and stealing floppy disks and CD-ROMS); Young, *supra* note 1, at 70. As Young illustrates the majority of vital corporate data is stored on computers and network servers with varying degrees of security. *Id.* at 73. Furthermore, Young illuminates the potential danger, "People do things in the computer environment that they would never do outside". *Id.* at 71. An example depicts this theory. *Id.* "Most people would not steal a car, but what about copying a customer database file or the internal pricing spreadsheet of a competitor?" *Id.* It is important to contrast competitive intelligence and illegal espionage. Competitive intelligence can be used both tactically and strategically. Crock, *supra* note 12, at 17. It borrows tools and methods from strategic planning, which takes a broad view of the market and how a particular company hopes to position itself. *Id.* at 17. Analysts study everything from rivals' new products and manufacturing costs to profiles of executives. *Id.* Competitive intelligence serves as a radar screen, spotting new opportunities or helping to

address the growing importance and significance of protecting trade secrets and proprietary information.²⁰ Moreover, the U.S. legal system must implement a powerful criminal deterrent to combat the simple, inexpensive and sophisticated methods of theft, which are virtually effortless to implement, but extremely difficult to detect.²¹

The theft of corporate trade secrets²² and proprietary information has largely been protected through the remedies availed in civil

avert disaster. *Id.* Competitive or corporate intelligence becomes illegal espionage when it involves the theft of proprietary information, materials, or trade secrets. *Id.* at 17. The distinction becomes difficult to ascertain given the potential to draw lines on ethical and legal grounds. Stealing price sheets from a corporate office would be both ethically wrong and illegal. However, expressing an interest in a job to find out a rival's new product plans may be devoid of ethics, but a gray area exists as to whether this is an illegal practice. To further confuse the issue, two authors have described various methods for stealing trade secrets ethically. See Weisner & Cava, *supra* note 16, at 1076. This Note does not attempt to explain or contradict the distinction between the ethical and legal aspects of competitive intelligence and illegal espionage. This Note devotes its attention to providing an adequate deterrent to preventing illegal espionage through actual theft of trade secrets and proprietary information.

²⁰ See *supra* notes 15-17 and accompanying text.

²¹ See *supra* notes 18-19 and accompanying text.

²² Trade secrets are, "any formula, pattern, device, or compilation of information which is used in one's business and which gives him an opportunity to obtain an advantage over competitors." RESTATEMENT (FIRST) OF TORTS § 757 (1939). In determining whether the proprietary information is protected by qualifying as a formula, pattern, device, or compilation of information, six factors are delineated by the Restatement:

(1) the extent to which the information is known outside of an individual's business; (2) the extent to which it is known by employees and others involved in his business; (3) the extent of measures taken by him to guard the secrecy of the information; (4) the value of the information to him and his competitors; (5) the amount of effort or money expended by him in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.

Id. For a further discussion of competing definitions of a trade secret, see Gale R. Peterson, *Trade Secrets in an Information Age*, 32 HOUS. L. REV 385, 389-92 (1995). Another influential definition of a trade secret, one adopted by numerous states in promulgating trade secret laws comes from the Uniform Trade Secrets Act (UTSA). *Id.* The UTSA defines a trade secret as follows:

information including a formula, pattern, compilation, program, device, method, technique, or process, that (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Uniform Trade Secrets Act §§ 1-11, 14 U.L.A. 438 (1985). The fundamental basis and intent of both definitions are similar as they both focus on the presence of value and competitive

litigation.²³ However, for numerous reasons, the remedies available to companies through civil litigation fail to provide the equivalent deterrent of criminal laws on theft of trade secrets by corporate spies.²⁴ First, the purpose of criminal sanctions is punitive and seeks to deter socially undesirable activity.²⁵ Criminal sanctions seek to provide a penalty with the goal of preventing the behavior from occurring in the future, while punishing the past behavior.²⁶ In contrast, civil law sanctions serve the purpose of compensation and returning the party to a preexisting status quo.²⁷ Second, criminal and civil sanctions produce different remedies.²⁸ Criminal sanctions place an inherent stigma on the individual, with punishment being the conventional device for the expression of attitudes of resentment and indignation.²⁹ Criminal sanctions produce a remedy of symbolic significance missing from other penalties.³⁰ Civil sanctions remedy the problem in an entirely different manner, most notably through monetary disbursements.³¹ Criminal law serves as a proactive

advantage while detailing secrecy requirements. Peterson, *supra* note 22, at 387-88. See *infra* Sections II and III for an analysis of federal and state criminal statutory law definitions of trade secrets.

²³ Corporations most frequently have two potential avenues under which to bring civil lawsuits. First, many businesses employ covenants not to compete, nondisclosure agreements and confidentiality agreements with their employees. David Cathcart, *Contracts with Employees: Covenants Not To Compete and Trade Secrets*, 36 ALI-ABA 87, 100 (1997). All three agreements are similar in substance and allow the company to bring a lawsuit for breach of contract or for breach of fiduciary duty if an employee discloses protected information. *Id.* Secondly, companies have the option of bringing a lawsuit for misappropriation of a trade secret under state tort law. *Id.* Over 40 states recognize the tort of misappropriation of trade secrets. Jonathan Band, *The Economic Espionage Act: Its Application in Year One*, CORP. COUNS., Nov. 1997, at 1. These states follow most aspects of the UTSA including its definition of trade secrets. See *supra* note 22. Utilizing this approach, the corporation can seek injunctive relief and monetary damages. See *infra* notes 24-33 detailing the advantages and disadvantages of civil law remedies.

²⁴ A succinct statement of the problem is that criminal liability is a far more effective deterrent than civil liability because "a long prison sentence puts the fear of God into people much more effectively than a slap on the wrist." Carol S. Steiker, *Punishment and Procedure: Punishment Theory and the Criminal-Civil Procedural Divide*, 85 GEO. L.J. 775 (1997).

²⁵ Kenneth Mann, *Punitive Civil Sanctions: The Middleground Between Criminal and Civil Law*, 101 YALE L.J. 1795, 1807 (1992).

²⁶ *Id.*

²⁷ *Id.*

²⁸ *Id.*

²⁹ Brent Fisse, *Reconstructing Corporate Criminal Law: Deterrence, Retribution, Fault and Sanctions*, 56 S. CAL. L. REV. 1141, 1147 (1983).

³⁰ *Id.* The "stigma theory" of criminal punishment is justified on three basis. First, the actor is blameworthy in causing the harm. *Id.* at 1148. Second, the harm is unwanted. *Id.* at 1147. Third, the stigma will have a deterrent effect on future behavior. *Id.*

³¹ Steiker, *supra* note 24, at 783. The nature of each sanction serves different purposes and corrects behavior through competing remedies. *Id.*

approach to deterring the problem before it occurs, while civil law serves to compensate the victim for activity that has harmed the individual.³² For these reasons, civil litigation serves important interests in this area other than deterrence.³³ However, compared to other intellectual property laws, civil trade secret laws have the potential to provide a more effective and comprehensive legal protection.³⁴ This dichotomous relationship has the potential to adequately protect corporations and businesses from theft and misappropriation of trade secrets through separate, but related remedies.³⁵ Civil trade secret laws provide an effective defensive approach, while criminal trade secret laws provide a powerful proactive deterrent to combat the growing simplicity and ease of theft.³⁶ However, while state civil trade secret laws and remedies in this area provide an effective defensive response, current state criminal

³² *Id.* at 784-86. Expanding on this theory, protecting trade secrets through civil litigation provides an effective defensive response. *Id.* Corporations may decline to pursue civil litigation because the financial resources, combined with the time and effort needed to investigate and bring the lawsuit, will produce civil penalties that are light, insignificant, and provide inadequate compensation relative to the loss incurred. *Id.* Civil litigation also suffers from three inherent drawbacks. *Id.* First, even with a civil law injunction, the secret information has been publicized. *Id.* Second, damage awards never fully compensate the victim, particularly when the individual thief is judgment proof. *Id.* Third, the primary focus during the civil lawsuit is on whether the information qualifies as a trade secret and becomes removed from the misconduct of the party. *Id.*

³³ Gerald Mossinghoff, *The Economic Espionage Act: A New Federal Regime of Trade Secret Protection*, 79 J. PAT. & TRADEMARK OFF. SOC'Y 191 (1997).

³⁴ Peterson, *supra* note 22, at 386. Contrasted with protection given to patents and copyrights, trade secret protection is immediate, unlimited in duration, and does not require government action in licensing or registration. *Id.* at 386. Furthermore, trade secret protection is broader, covering a variety of information that is not explicitly covered under patent, copyright, or trademark protection. *Id.* Examples of information that would classify as a trade secret, but not a patent, copyright, or trademark include marketing plans, financial information, customer and supplier lists, designs, drawings, and technological strategies. *Id.* The U.S. Supreme Court has upheld trade secret laws against a claim of preemption by federal patent law. *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 491-93 (1974). For a more detailed analysis see Epstein & Levi, *supra* note 14, at 887. As these authors point out, the trade secret process is cheaper and quicker to implement than the patent process. *Id.* Furthermore, unlike patent law, there is no subject matter requirement to obtain trade secret protection, thus creating more flexibility and expanded coverage and protection. *Id.* at 888. Finally, for most corporations trade secret protection allows the information to remain confidential, which is a better strategy than publicizing the information through use of a patent or copyright. See generally Cindy Collins, *Trade Secrets: The Economic Espionage Act, Friend or Foe?*, INSIDE LITIGATION, Sept. 1997, at 14.

³⁵ See *supra* notes 22-34.

³⁶ See *supra* notes 22-34.

trade secret laws fail to provide an effective deterrent to the theft and misappropriation of trade secrets.³⁷

The main objective of this Note is to propose an effective legal method to deter the theft of trade secrets and proprietary business information using the criminal justice system of both the federal and state courts.³⁸ Section II of this Note details the various criminal law sanctions and penalties under current federal statutory law, including the recently promulgated Economic Espionage Act of 1996 (EEA).³⁹ This Section also briefly details the judicial interpretation of these various federal statutes.⁴⁰ Furthermore, this Section discusses various practical problems and illustrates the weaknesses of addressing these problems through federal government intervention.⁴¹

Section III of this Note evaluates the current state criminal law approaches regarding trade secret theft, including an analysis of the sanctions and penalties currently in effect.⁴² Unfortunately, most of the current state law approaches (for different reasons than current federal law) are inadequate, outdated, and lack sufficient deterrence to combat the dangers and importance of protecting trade secrets and corporate proprietary information.⁴³ Section IV of this Note proposes a response to these problems by creating a model criminal penal code combining the strongest aspects of the EEA and state law statutory approaches to create powerful criminal sanctions which will provide the best possible deterrent effect on corporate spies in America.⁴⁴ This tool will provide the states that have not adopted any criminal statutes regarding the theft

³⁷ See *infra* Section III.

³⁸ This is complicated naturally by many practical aspects discussed in *supra* notes 18-19. The problem is two-fold. "American companies are like innocent children in the forest. They have no idea how many wolves are after them." Yates, *supra* note 13, at B1. The more troubling aspect is that many companies are not ignorant, but arrogant. *Id.* This has been described as the "head in the sand approach". *Id.* Many companies are simply not willing to look at it because they do not think they are targets. *Id.* While a model criminal penal code will not solve all of these problems directly, an effective criminal deterrent approach is far superior to the current legal protection available to corporations. See *infra* Section IV.

³⁹ 18 U.S.C.A. §§ 1831-1839 (West Supp. 1998). See *infra* notes 95-117 and accompanying text.

⁴⁰ See *infra* notes 61-73, 79-84 and accompanying text.

⁴¹ See *infra* notes 107-17 and accompanying text.

⁴² See *infra* Section IIIB.

⁴³ See *infra* Section IIIC.

⁴⁴ See *infra* Section IV.

of trade secrets a viable, detailed, and illustrative model to assist in passing legislation.⁴⁵

II. FEDERAL STATUTORY APPROACH TO THE PROTECTION OF TRADE SECRETS

A. Introduction

Prior to 1996, federal prosecutors attempted to use a patchwork of three federal statutes to prosecute individuals for theft or misappropriation of trade secrets and confidential business information.⁴⁶ However, all three federal statutes, The Interstate Transportation of Stolen Property Act (ITSA),⁴⁷ Wire Fraud statutes,⁴⁸ and Mail Fraud statutes⁴⁹ were clearly not originally designed to cover trade secrets and proprietary business information.⁵⁰ In 1996, Congress attempted to remedy the problem by providing a comprehensive federal statute directly addressing the theft of trade secrets and confidential business information entitled the Economic Espionage Act (EEA).⁵¹ This Section will detail the development and application of each federal statute to the theft of trade secrets and confidential business information.

⁴⁵ Furthermore, this tool will allow states that currently have some form of criminal law protection to amend their outdated and ineffective statutes.

⁴⁶ See generally James Pooley et al., *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177 (1997); Stanley S. Arkin & Michael F. Colosi, *The Criminalization of Theft of Technology and Trade Secrets*, 3 No. 5 BUS. CRIMES BULL. 4 (1996). One distinct and limited federal statute provides criminal sanctions for the unauthorized disclosure of government information by a government employee. 18 U.S.C. § 1905 (1994). While this statute does explicitly cover trade secrets, the usefulness of this statute is limited in two regards. First, the statute specifically covers only government employees who disclose or misappropriate only government information. *Id.* Therefore, this statute does not apply to private individuals, corporations, or foreign governments. *Id.* In addition to the limited scope, the statute only provides for misdemeanor criminal sanctions and is seldom used for prosecution purposes. Pooley, *supra* note 46, at 229. In fact, only one appellate decision has been reported under this statute. See *United States v. Wallington*, 889 F.2d 573 (5th. Cir. 1989) (upholding a conviction for running background checks whom a friend of the defendant suspected of drug dealing).

⁴⁷ 18 U.S.C. § 2314 (1994). See *infra* notes 52-75 and accompanying text.

⁴⁸ 18 U.S.C. § 1343 (1994). See *infra* notes 76-84 and accompanying text.

⁴⁹ 18 U.S.C. § 1341 (1994). See *infra* notes 76-84 and accompanying text.

⁵⁰ Pooley, *supra* note 46, at 177. Generally all three statutes prohibit the theft and misappropriation of property. Toren, *supra* note 15, at 64. Case law recognizes that under certain circumstances these federal statutes may encompass the theft of trade secrets and confidential business information. *Id.* See *infra* notes 52-94 and accompanying text for a detailed examination and analysis of each federal statute and case law interpreting the statutes to cases involving theft of trade secrets and proprietary business information.

⁵¹ 18 U.S.C.A. §§ 1831-1839 (West 1996). See *infra* notes 94-120 and accompanying text.

B. *The Interstate Transportation of Stolen Property Act: 18 U.S.C. § 2314 (ITSA)*

The first of these statutes, the ITSA, was enacted in 1934 pursuant to the Commerce Clause of the Constitution, with the goal of aiding states in the detection and punishment of criminal activity.⁵² Under this statute the government is required to prove two preliminary elements to obtain a conviction.⁵³ First, the government must prove that the trade secrets were transported in interstate or foreign commerce.⁵⁴ Second, the government must prove that the defendant knew that the information was stolen, converted or taken by fraud.⁵⁵ Next, the government must also show that the value of the trade secret exceeds five thousand dollars.⁵⁶ Finally, to obtain a conviction, the government must prove that the trade secret or confidential business information constitutes a "good, ware, or merchandise," a requirement under the language of the statute.⁵⁷

⁵² Toren, *supra* note 15, at 68. As Toren explains, the statute specifically addressed the growing problem of criminals evading state authorities by fleeing across state lines with stolen property. *Id.* As the title of the act illustrates, its application is limited to transportation in interstate commerce and does not apply to intrastate misappropriation and theft. *Id.* The statute provides, in pertinent part:

Whoever transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of \$5000 or more, knowing the same have been stolen, converted or taken by fraud...shall be fined under this title or imprisoned not more than [a number of years], or both.

18 U.S.C. § 2314 (1994).

⁵³ Toren, *supra* note 15, at 68.

⁵⁴ *Id.*

⁵⁵ *Id.* These two inquiries generally do not provide any difficult legal questions. *Id.*

⁵⁶ Toren, *supra* note 15, at 81. This requirement is not always easy to establish for two reasons. *Id.* at 82. First, the market value of a trade secret is frequently not ascertainable. *Id.* Second, trade secrets are often stolen at a developmental stage when the information has never been sold or marketed. *Id.* No uniform approach has developed, but courts have developed three common methods for determining value. *Id.* at 84. One method employed takes into consideration the costs to develop the trade secret. See *United States v. Stegora*, 849 F.2d 291 (8th Cir. 1988). Another method considers the market in which the trade secrets change hands among thieves. See *United States v. Lester*, 282 F.2d 750 (3d Cir. 1960). Finally, the company who developed the trade secret can show the potential revenues or profits that would be generated by the product, service, or process. See *United States v. Greenwald*, 479 F.2d 320 (6th Cir. 1973), *cert. denied*, 414 U.S. 854 (1973). See generally Toren, *supra* note 15, at 84.

⁵⁷ 18 U.S.C. 2314 (1994). See *infra* notes 58-74 and accompanying text.

The theft of a tangible trade secret triggers the statute.⁵⁸ Furthermore, if an intangible trade secret is embodied in a tangible item that is stolen, the statute is also triggered.⁵⁹ However, the main drawback to the application of this statute to the theft of trade secrets is illustrated by its treatment of purely intangible property.⁶⁰ In particular, the decision in *United States v. Brown*⁶¹ casts doubts on whether the

⁵⁸ *United States v. Seagraves*, 265 F.2d 876 (3d Cir. 1959). In *Seagraves*, the defendant purchased numerous Gulf Oil Corporation geophysical and geological maps (revealing the potential locations for productive oil wells) from an employee of the company who had stolen the maps. *Id.* at 878. The court held that the maps fell under the language "goods, wares and merchandise" of 18 U.S.C. § 2314. *Id.* at 880. The court reasoned that the maps involved were frequently sold, possessed significant value, and the information was not generally known; therefore, they classified the maps as a trade secret. *Id.* See also *United States v. Belmont*, 715 F.2d 459, 463 (9th Cir. 1983) (holding that interstate sales of pirated videotape cassettes violates 18 U.S.C. § 2314). These cases demonstrate that the theft of a physical object containing the actual trade secret or confidential information will qualify for prosecution under this act. Pooley, *supra* note 46, at 184.

⁵⁹ *United States v. Bottone*, 365 F.2d 389 (2d Cir. 1966). In *Bottone*, the defendant temporarily removed and copied confidential documents detailing a laboratory manufacturing process. *Id.* at 391. The defendant argued that photocopies, microfilms, and notes did not constitute "goods, wares or merchandise," under the statute as the tangible product was not actually stolen. *Id.* at 393. The court held that stolen intangible information embodied and transported in a different physical object fell under the language of "goods, wares or merchandise." *Id.* The court reasoned that the subject matter and substance of the information should be protected, whether or not the physical form of the stolen tangible object was possessed by the original owner. *Id.* at 394. The court left open for question the possibility that the statute might not be triggered if no tangible objects were taken. For example, a secret formula could be memorized or carried away in the recesses of a thievish mind and placed in writing at a subsequent time. *Id.* at 393. The problem of protecting purely intangible secrets under this statute has conflicting results. See *infra* notes 60-75 and accompanying text. However, other courts have followed *Bottone* and found that when the physical form of stolen goods is secondary in every respect to the matter recorded in them, transformation of information in stolen papers to an intangible object never possessed by the original owner is covered by the statute. See, e.g., *United States v. Greenwald*, 479 F.2d 320 (6th Cir. 1973), *cert. denied*, 414 U.S. 854 (1973) (holding that stolen copies of documents containing manufacturing formulations of chemical products transported in interstate commerce constituted goods, wares, and merchandise under 18 U.S.C. § 2341).

⁶⁰ Intangibles are often defined as "property...lacking physical existence". BLACK'S LAW DICTIONARY 558 (6th ed. 1991). As trade secrets often constitute purely intangible property or quasi-intangible property, this is extremely problematic and signifies the main weakness with using this statute to prosecute the theft of trade secrets. Pooley, *supra* note 46, at 180. The ITSA was drafted at a time when information could not be quickly copied and instantaneously transmitted to any location in the world. *Id.* Furthermore, intangible information currently plays a much greater significance to individual companies in the micro, and the economy as a whole in the macro, than it did when the ITSA was promulgated. *Id.* See *supra* notes 15-16 discussing the intangible nature of trade secrets and proprietary information.

⁶¹ 925 F.2d 1301 (10th Cir. 1991).

phrase, "goods, wares, and merchandise" contained in the statute covers intangible property.⁶² The defendant in *Brown* worked as a computer programmer for The Software Link, Inc. (TSL).⁶³ The company suspected Brown of theft of computer programs and source code.⁶⁴ After an FBI investigation produced evidence that the defendant had stolen the source code to a TSL product, the defendant was indicted pursuant to 18 U.S.C. § 2314.⁶⁵ However, the court determined that purely intangible property cannot constitute "goods, wares or merchandise" within the meaning of the statute.⁶⁶ The court reasoned that under

⁶² The key question arises as to whether the phrase "goods, wares or merchandise" in the statute requires a strict application by the courts to theft of only tangible items. See *supra* notes 58-60 and accompanying text. One federal district court has refused to read a tangibility requirement into the statute. *United States v. Riggs*, 739 F. Supp. 414 (N.D. Ill. 1990). In *Riggs* two defendants developed a scheme to steal Bell South's computer text file which contained information regarding its enhanced 911 (E911) system for handling emergency calls. *Id.* at 417. The text file detailed the procedures for installation, operation, and maintenance of E911 services. *Id.* Bell South considered this computer file to contain valuable proprietary information and closely guarded the information from public disclosure. *Id.* The defendants stole this information through the transmission of electronic impulses from the Bell South computer to the defendant's computer. *Id.* at 420. The defendant argued that the proprietary information contained in the computer text file did not constitute a "good, ware or merchandise" within the purview of the statute. *Id.* The defendant argued that no tangible objects were stolen from Bell South, thereby distinguishing cases where intangible information was embodied in tangible objects and then stolen. *Id.* at 421. See *supra* note 58 and accompanying text discussing cases involving this theory. The court held that tangibility is not a requirement to meet the "goods, wares or merchandise" test of 18 U.S.C. § 2314. *Id.* The court reasoned that although the information is stored inside a computer and is therefore purely intangible, the information is in a transferable, accessible, and salable form. *Id.* The court further reasoned that reading a tangibility requirement into the definition of "goods, wares or merchandise" would unduly restrict the scope of § 2314, especially in this modern technological age. *Id.* The court stressed the notion that prior cases have liberally construed the terms in the statute to designate property which is ordinarily the subject of commerce. *Id.* However, a federal appeals court in *United States v. Brown* explicitly rejected the reasoning of *Riggs* and held that a tangibility requirement must be present for successful prosecution under § 2314 *Brown*, 925 F.2d at 1308-9. See *infra* notes 63-75 and accompanying text.

⁶³ *Brown*, 925 F.2d at 1302. One asset of TSL was a computer program which allowed IBM "compatible computers to perform complex activities such as multi-tasking and sharing of data among multiple users." *Id.* at 1302 n.2.

⁶⁴ *Id.* at 1303. Source code is frequently referred to as the "assembly language" in which programmers write the computer programs. *Id.* at 1303 n.4. The code is then translated into machine language and incorporated into the computer system. *Id.* The defendant eventually became the subject of an FBI investigation which culminated in the issuance and execution of a search warrant. *Id.* at 1302.

⁶⁵ *Id.* at 1303.

⁶⁶ *Brown*, 925 F.2d at 1309. The court cited with approval the notion that if intangible property can be represented physically or in a tangible medium (such as photocopying or writing the information on a piece of paper), then the object qualifies as a good, ware or

*Dowling v. United States*⁶⁷ the element of physical tangibility in the stolen item is required for a trade secret to be covered under the "goods, wares, or merchandise" language in section 2314.⁶⁸ Therefore, the court explicitly required that for information to constitute a "good, wares or merchandise" under the statute, the information must be embodied in a tangible object or medium.⁶⁹ In an increasingly electronic environment, where a thief can transmit stolen trade secrets without misappropriating any tangible property owned by the victim, the viability of section 2314 is seriously in question.⁷⁰ In cases where no tangible property is stolen,

merchandise. See *supra* note 59. Also, a tangible item qualifies for application of § 2314. *Brown*, 925 F.2d at 1308-1309. See *supra* note 58. However, the court distinguished this case from the prior cases as they involved situations where there existed a physical identity between the intangible item and the unlawfully obtained and transported tangible object. *Brown*, 925 F.2d at 1307-1309. In this case, the prosecution could not prove physical theft or transportation of any physical property belonging to TSL. *Id.*

⁶⁷ 473 U.S. 207 (1985). The Supreme Court in *Dowling* was confronted with a prosecution for interstate distribution of bootlegged Elvis Presley records in violation of 18 U.S.C. § 2314 (1994). *Id.* at 209. While the case involved copyright infringement, the court set forth critical language in the context of trade secret protection under the ITSA. The Court stated that prosecution under ITSA required a "physical identity between the items unlawfully obtained and those ... transported, and hence some prior physical taking of the subject goods." *Id.* at 216. This language allowed the *Brown* court to hold that purely intangible property, such as the source code discussed in *supra* note 64 is not covered under 18 U.S.C. § 2314 (1994). *Brown*, 925 F.2d at 1307.

⁶⁸ *Brown*, 925 F.2d at 1309. The court stated that "The computer program itself is an intangible intellectual property, and as such, it alone cannot constitute goods, wares, merchandise...within the meaning of §§ 2-314 or 2-315." *Id.* On the surface other courts have reached different outcomes. See *United States v. Seagraves*, 265 F.2d 876 (3d Cir. 1959); *United States v. Lester*, 282 F.2d 750 (3d Cir. 1960). However, these cases are easily distinguished in that the stolen intangible item was represented in a tangible object that was transported in interstate commerce. Toren, *supra* note 15, at 76. Therefore, *Brown* remains as the only case involving theft of purely intangible property prosecuted under the ITSA. *Id.* at 81. Furthermore, a recent 7th Circuit case affirmatively states that "we are not aware of any case applying any portion of 18 U.S.C. § 2314 to something completely intangible." *United States v. Kenngott*, 840 F.2d 375, 380 (7th Cir. 1987).

⁶⁹ *Id.* See also *United States v. Greenwald*, 479 F.2d 320 (6th Cir. 1973), *cert. denied*, 414 U.S. 854 (1973); *Hancock v. Decker*, 379 F.2d 552 (5th Cir. 1967); *United States v. Seagraves*, 265 F.2d 876 (3d Cir. 1959); *United States v. Lester*, 282 F.2d 750 (3d Cir. 1960); *United States v. Kenngott*, 840 F.2d 375, 380 (7th Cir. 1987); *United States v. Bottone*, 365 F.2d 389 (2d Cir. 1966). Most importantly the language in *United States v. Dowling*, 473 U.S. 207 (1985) clearly contemplates a physical connection or physical taking of a tangible object. Toren, *supra* note 15, at 81. See *supra* notes 58-60 and accompanying text.

⁷⁰ Pooley et al., *supra* note 46, at 185. This illustrates the first problem with the ITSA, limited scope. See *supra* notes 15-16, discussing the primary feature of trade secrets and proprietary business information as encompassing intangible aspects. Another problem with this interpretation of the statute is that it treats two defendants (both who misappropriated the same trade secret) differently depending on the mode of theft. Pooley et al., *supra* note 46, at 185. If the defendant steals the information by copying it and storing

prosecutors could no longer invoke section 2314.⁷¹ Therefore, the decision in *Brown* severely limits any prosecution for theft of trade secrets via computer technology.⁷² Also this decision could potentially be applied to many other sophisticated methods of electronic theft such as wireless microphones and electronic surveillance equipment where nothing tangible is removed from the company.⁷³

Furthermore, the language of *United States v. Dowling*⁷⁴ and *United States v. Brown*⁷⁵ is likely to have an adverse impact on the decision by the government as to whether to prosecute a case using this statute.⁷⁶ For these reasons, the impact of The Interstate Transportation of Stolen Property Act on deterring the misappropriation and theft of trade secrets and confidential business information is relatively minimal.⁷⁷ Other

it in a tangible medium, such as a computer disk, the statute applies. *Id.* at 184-85. If the thief follows the method of the defendant in *Brown* and transfers the information to another intangible medium, the statute arguably is not triggered. *Id.* These "short-comings" reveal the reasons for congressional decision to enact the Economic Espionage Act of 1996. *Id.* at 185. See *infra* notes 98-120 and accompanying text.

⁷¹ *Id.* Pooley et al., *supra* note 46, at 185.

⁷² *Id.*

⁷³ *Id.* See *supra* note 19 and accompanying text.

⁷⁴ 473 U.S. 207 (1985).

⁷⁵ 925 F.2d 1301 (10th Cir. 1991).

⁷⁶ Toren, *supra* note 15, at 81. Toren argues that the importance of these cases calls for an amendment to this statute to specifically include interstate transportation of stolen intangible property. *Id.* However, the passage of the Economic Espionage Act of 1996, discussed in *infra* notes 98-120, eliminates the need for any change to this statute.

⁷⁷ The problem is two-fold. S. REP. NO. 104-359, at 6 (1996). First, the statute deals specifically with crimes involving traditional goods, wares and merchandise. *Id.* And for this purpose, the statute has served its purpose extremely well. *Id.* However, this statute is not well suited to deal with situations involving "intellectual property" and intangible property. H.R. REP. NO. 104-788, at 10 (1996). As witnessed by the language of *Dowling* and *Brown*, discussed in *supra* notes 62-75, the trend of the courts in interpreting this statute to trade secrets and business information has failed to find that this type of property is covered under the ITSA. The current case law, therefore, limits the usefulness of prosecution under this statute. S. REP. NO. 104-359, at 6 (1996). Second, the statute was drafted at a time when no one contemplated the widespread use of computers and copy machines as a means of transferring information. *Id.* This is a corollary limitation similar to the lack of scope. Information can be wrongfully duplicated and transmitted electronically creating an intangible theft that would not be covered under this statute. *Id.* The goal and provisions of this statute were not meant to cover trade secrets and business information. *Id.* See *supra* notes 62-78 for discussion of the narrow scope problem, and *supra* note 52 for a discussion of the nature of the purpose and goal of this statute, detailing the lack of intent for coverage of trade secrets under this statute.

federal statutory approaches have encountered the same inherent difficulties as those witnessed by this statute.⁷⁸

C. *Federal Mail and Wire Fraud: 18 U.S.C. § 1341 & 18 U.S.C. § 1343*

The federal Mail Fraud and Wire Fraud statutes generally proscribe any scheme devised to obtain property by false or fraudulent means.⁷⁹ In one regard, convictions are easier to obtain under these statutes than The Interstate Transportation of Stolen Property Act⁸⁰ because of the

⁷⁸ Most notably all federal statutory law prior to the passage of the EEA was not directly aimed at the protection of trade secrets and proprietary business information. H.R. REP. NO. 104-788, at 12 (1996). As discussed *supra* note 52, the ITSA had a stated purpose of deterring transportation of stolen goods. As discussed in *infra* notes 83-84, both mail and wire fraud are limited by the mode of transportation. Therefore, when looking at the prior federal statutory scheme to prosecute theft of trade secrets (before the EEA), each statute suffers from different limitations which severely curtail any significant attempts at successful prosecution. The problem arises by trying to manipulate and extend the language and meaning of statutes that were never meant to address the specific problem at issue. As a result, prosecutors have had trouble "shoe-horning" economic espionage cases into these laws. S. REP. NO. 104-359, at 7 (1996). The EEA was promulgated to directly address the issue of theft and misappropriation of trade secrets. See *infra* notes 95-97 detailing the legislative history and purpose of the EEA.

⁷⁹ 18 U.S.C. § 1341, provides, in pertinent part:

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, or to sell, dispose of, loan, exchange, alter, give away, distribute, supply, or furnish or procure...for the purpose of executing such scheme or artifice...places in any post office or authorized depository for mail, any matter or thing whatever to be sent or delivered by the Postal Service, or deposits or causes to be deposited any...thing...to be sent or delivered by any private or commercial interstate carrier, or takes or receives therefrom, any such matter or thing, or knowingly causes to be delivered by mail or such carrier...shall be fined under this title or imprisoned not more than five years or both.

18 U.S.C. § 1341 (1994).

18 U.S.C. § 1343 provides in pertinent part:

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio or television communication in interstate or foreign commerce...shall be fined under this title or imprisoned not more than five years, or both.

18 U.S.C. § 1343 (1994). Both statutes raise the penalty to not more than 30 years imprisonment and a one million dollar fine if the violation affects a financial institution. 18 U.S.C. §§ 1341, 1343. (1994)

⁸⁰ 18 U.S.C. § 2314 (1994).

expansive language used in the statutes.⁸¹ The broad reach of these statutes as applied to trade secrets and proprietary business information is illustrated by *Carpenter v. United States*.⁸² In *Carpenter*, the Supreme Court held that an employee's use of the confidential information generated by his employer violated both section 1341 and section 1343.⁸³ The Court specifically recognized that the unlawful use of the Wall Street Journal's confidential business information is within the reach of both federal Mail Fraud and Wire Fraud statutes.⁸⁴ Furthermore, the Court found that although the nature of WSJ property right was intangible, the scope of protection under both statutes is not limited only to tangible property rights.⁸⁵ However, the mail fraud and wire fraud statutes

⁸¹ Pooley et al., *supra* note 46, at 185. The broader scope results from distinguishing the narrower phrase "goods, wares, and merchandise" as used in § 2314 and the term "property" used in sections 1341 and 1343. *Id.* As discussed in *supra* notes 60-72, intangible information has difficulty falling under the language of "goods, wares and merchandise" of § 2314. However, courts have repeatedly found that the term "property" encompasses intangible property. See *United States v. Seidlitz*, 589 F.2d 152 (4th Cir. 1978). In *Seidlitz* the defendant was prosecuted for transmitting computer information from a company called OSI via the telephone. *Id.* at 155. The court deemed the intangible information a property right possessed by OSI. *Id.* at 160. The court reasoned that the company invested massive sums of money to develop and modify the system and enjoyed a huge competitive advantage as a result of these efforts. *Id.* The court further guaranteed protected status because the property was not in the public domain. *Id.* The situation is nearly identical to the prosecution of the defendant in *Brown*. *Brown*, 925 F.2d at 1301. However, the court interpreting *Brown* failed to allow protection for intangible property under § 2314. *Id.* In this case, the broader term "property" allows prosecutions that may escape § 2314 through the use of mail and wire fraud statutes. Pooley et al., *supra* note 46, at 185.

⁸² 484 U.S. 19 (1987).

⁸³ The defendant was an author of an advice column for the *Wall Street Journal* (WSJ). *Carpenter*, 484 U.S. at 19. The defendant entered into a scheme with stockbrokers to exchange confidential information in the column in advance of publication. *Id.* In return, the defendant would receive a portion of the profits. *Id.* The advice column written by the defendant had a qualitative impact on the market prices of the stocks it discussed because of its perceived quality and integrity. *Id.* On the basis of this scheme, the defendants were convicted of violating insider trading laws. *Id.* More importantly to this discussion, the court upheld their convictions based on 18 U.S.C. § 1341 and 18 U.S.C. § 1343. *Id.*

⁸⁴ *Carpenter*, 484 U.S. at 19. The court acknowledged that the WSJ had a "property right in keeping confidential and making exclusive use, prior to publication, of the...contents of the column." *Id.* Therefore, the Supreme Court has afforded protection under these statutes to confidential business information and trade secrets. *Id.*

⁸⁵ The defendants attempted to assert that their activities were not a scheme to defraud the WSJ within the meaning of the statute, because the rights asserted by the WSJ are intangible rights and therefore outside of the scope of the statutes. *Id.* at 25. The court explicitly rejected this assertion. *Id.* The Court found that the event which defrauded WSJ was not selling the information to a competitor. *Id.* The fraud involved was that the WSJ was deprived of its right to exclusive use of the information. *Id.* at 26. The business has a right to decide how to use the information prior to publication, and the defendant's

critically suffer from one weakness: trade secret theft generally does not involve the use of interstate mail or wire.⁸⁶ Therefore, although these statutes have a broader scope, they do not adequately address the problems demonstrated by the most common and prevalent types of corporate and economic espionage.⁸⁷

Prior federal law in the area of the theft and misappropriation of trade secrets and proprietary business information provides no useful statutory deterrent.⁸⁸ The ITSA suffers from an extremely limited scope in the type of information protected.⁸⁹ This statute never contemplated the massive importance and widespread use of purely intangible information in the current global economy.⁹⁰ The federal Mail and Wire

interference with that right, whether intangible or not, does not make the information any less protected. *Id.* at 25.

⁸⁶ Pooley et al., *supra* note 46, at 186. Furthermore, as illustrated by the *Carpenter* decision, the prosecution must also establish an intent to defraud on the part of the defendants. *Carpenter*, 484 U.S. at 19.

⁸⁷ See *infra* notes 88-92. An easy way to avoid prosecution is not to transmit the information through the mail or by wire. The quickest way to transmit the information remains by meeting face to face. The thief and potential purchaser of the information can personally meet, discuss the terms of the deal, and transfer the stolen information without any threat of prosecution under these statutes. While the broader scope helps alleviate the problem under the ITSA, the limitation on the mode of transmittal of the information curtails any meaningful deterrent threat under these statutes.

⁸⁸ Although Congress has enacted both patent and copyright protection, no federal law prior to the EEA protected proprietary economic information from theft and misappropriation in a systematic and principled manner. S. REP. NO. 104-359, at 6-7 (1996). See *supra* notes 15-17 for a discussion of the value of proprietary economic information to the lifeblood of U.S. corporations and the economy. See *infra* notes 98-120 for a discussion of the EEA, discussing the improvements and advantages made by this statute to the protection of trade secrets through criminal penalties, but also detailing the many inherent and external limitations present in this statute.

⁸⁹ See *supra* notes 60-78 and accompanying text.

⁹⁰ As discussed, intangible assets have become critically important to the prosperity of companies. See *supra* note 15-16. See H.R. REP. NO. 104-788, at 7 (1996). To demonstrate this point, in 1982 tangible assets (machinery, equipment, buildings, land) accounted for 62% of the market value of mining and manufacturing companies. *Id.* By 1992, they represented only 38% of the market value. *Id.* This survey is interesting in two regards. First, the data illustrates the shifting nature of the asset base. This illuminates that in the future, growth and stability comes not from advancements and augmentation to the tangible asset base, but to achieving economic growth and value through the exploitation of intangible assets. This exploitation is accomplished by keeping the information confidential and secret. Second, intangible assets are less prevalent in manufacturing companies relative to biotechnology companies and other "high-tech" industries. As the nation moves into an economy based more on information and technology and less dependent on manufacturing firms, the value and importance of intangible assets will only continue to grow. Protection of these valuable rights requires principled, independent,

Fraud Statutes fail to adequately deter theft and misappropriation by severely limiting the modes of transfer that trigger prosecution.⁹¹ This statute was not designed to combat the highly sophisticated methods currently available for stealing trade secrets and business information.⁹² The patchwork nature of these statutes detailing protection against the theft and misappropriation of trade secrets and business information, combined with the indirect nature of criminal prosecution under these laws, led Congress to directly address the problem with acclaimed legislation in 1996.⁹³

Congressional hearings prior to enactment of the Economic Espionage Act of 1996 amply document the two major underpinnings of the legislation.⁹⁴ First, foreign powers, through a variety of means, are actively involved in stealing critical technologies, data and information from U.S. companies for the economic benefit of their own industrial sector.⁹⁵ Second, laws on the books, including the Interstate Transportation of Stolen Property Act and the Mail Fraud and Wire Fraud statutes were of virtually no use in prosecuting acts of economic espionage.⁹⁶ Therefore, Congress responded to these dual concerns by passing The Economic Espionage Act of 1996.⁹⁷

powerful, and systematic statutory protection through both federal criminal law and state criminal and civil law.

⁹¹ The act has proved limited in use mainly because the statute requires proof that the mail system or wire system are used in commission of the act. H.R. REP. NO. 104-788, at 10 (1996). See *supra* notes 86-87 and accompanying text.

⁹² See *supra* note 19. The majority of theft and misappropriation of trade secrets and confidential business information fails to involve mail or wire transfers. See *supra* note 87.

⁹³ As President Clinton succinctly stated in signing the EEA into law, "Until today, federal law has not accorded appropriate or adequate protection to trade secrets. Law enforcement officials relied...on antiquated laws that have not kept pace with the technological advances of modern society." Statement of the President of the United States, 1996 U.S.C.C.A.N. 4034 (Oct. 11, 1996). See *infra* notes 98-120 discussing the EEA, its purpose, scope, penalties and deterrence effect.

⁹⁴ Mossinghoff, *supra* note 33, at 191.

⁹⁵ *Id.* at 193. Robert Gates, former director of the CIA states before Congress, "Many foreign intelligence services are shifting the emphasis in targeting to...economic information and technology as opposed to military information." S. REP. NO. 104-359, at 5 (1996). One author has written an entire book on the subject of foreign espionage of U.S. companies' proprietary economic, business and technological information. FIALKA, *supra* note 12. See also *supra* note 12 discussing foreign government sponsorship of economic espionage. Not only are foreign governments responsible for theft of trade secrets and confidential business information, U.S. corporations are also to blame. See *supra* notes 12-13.

⁹⁶ Mossinghoff, *supra* note 33, at 193.

⁹⁷ 18 U.S.C.A. §§ 1831-1839 (West 1996).

D. *The Economic Espionage Act of 1996 (EEA)*

The EEA provides an extremely comprehensive definition of what constitutes a trade secret.⁹⁸ The definition generally tracks the definition of trade secrecy in the UTSA.⁹⁹ However, the language of the EEA is different in three important aspects.¹⁰⁰ First, the EEA expands the list of potential types of trade secrets and confidential business information.¹⁰¹ Second, the EEA extends the definition of trade secrets to include both tangible and intangible information.¹⁰² Third, the EEA enlarges the

⁹⁸ The term "trade secret" means:

All forms and types of financial, business, scientific, technical, economic, or engineering information including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:

(A) the owner thereof has taken reasonable measures to keep such information secret, and

(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by the public.

18 U.S.C.A. § 1839 (West 1996). At the outset, this definition incorporates three extremely important concepts not covered by prior federal law. The definition specifically recognizes intangible property as a protected trade secret. *Id.* Second, the statute addresses the problem of thieves memorizing the information and transmitting that information at a subsequent time in the future. *Id.* Third, the economic value can be demonstrated by a showing that keeping the information secret could produce value in the future, i.e. the confidential information has a potential value, although not currently realized. *Id.*

⁹⁹ Pooley et al., *supra* note 46, at 188. See *supra* note 22 for the UTSA definition. However, the UTSA provides for remedies in civil litigation as opposed to criminal sanctions. The EEA definition is the first federal criminal statute to directly address the concerns of trade secret protection through a proactive deterrent, as opposed to a reactive remedy. See *supra* notes 94-98.

¹⁰⁰ Pooley et al., *supra* note 46, at 189.

¹⁰¹ *Id.* As representative of this expansion, section 1839 explicitly includes "financial, business [or] economic...information...." *Id.* Furthermore, section 1839 includes "plans...methods...processes, [and] programs...." *Id.* The language appears to be deliberately broad, to effectuate the legislative purpose and goal of providing a "comprehensive approach". S. REP. NO. 104-359 at 7 (1996).

¹⁰² The language explicitly encompasses information in any form "whether tangible or intangible." 18 U.S.C.A. § 1839 (West 1996). The importance of this language cannot be understated. The statute protects information in tangible objects and intangible information embodied in tangible objects (photocopying a supplier list from a computer screen). This is no great breakthrough, for, the court decisions under the ITSA covered this type of theft. See *supra* notes 58-60. However, the EEA covers information "stored in an individual's head." Pooley et al., *supra* note 46, at 189. Memorizing a trade secret equates to misappropriating a trade secret. *Id.* In theory, this would be somewhat difficult for the prosecution to prove, however; many civil suits have been successful under this theory. See

prohibited conduct with a comprehensive definition of misappropriation.¹⁰³

The EEA criminalizes both economic espionage by foreign entities¹⁰⁴ and the theft of trade secrets by domestic entities.¹⁰⁵ The provisions of

Stampede Tool Warehouse Inc. v. May, 651 N.E.2d 209 (Ill. App. Ct. 1995) (suit arising out of an employee memorizing customer lists).

¹⁰³ The act covers theft through obvious physical methods, such as "tak[ing], carry[ing] away, or conceal[ing]..." 18 U.S.C.A. §§ 1831, 1832 (West Supp. 1998). However, the act also defines misappropriation to include less conspicuous (and more difficult to detect) methods, such as "download[ing], upload[ing], destroy[ing]...replicat[ing]...communicat[ing]." *Id.* This definition closely follows to the UTSA. Again, the striking difference is in the approach. The EEA provides criminal sanctions, whereas the UTSA provides civil remedies. See *supra* notes 24-33.

¹⁰⁴ 18 U.S.C.A. § 1831 provides, in pertinent part:

(a) Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly:

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;

(3) receives, buys, or possesses a trade secret; knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in any of paragraphs (1) through (3); or

(5) conspires with one or more persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined not more than \$500,000 or imprisoned not more than 15 years, or both.

(b) Organizations: Any organization that commits any offense described in subsection (a) shall be fined not more than \$10,000,000.

18 U.S.C.A. § 1831 (West 1996).

Section 1839 defines the term "foreign instrumentality":

Any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government.

18 U.S.C.A. § 1839 (West 1996).

The term "foreign agent" means any officer, employee, proxy, servant, delegate, or representative of a foreign government. *Id.*

¹⁰⁵ 18 U.S.C.A. § 1832 provides, in pertinent part:

(a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the

this statute reprimand both illegal and immoral business conduct.¹⁰⁶ The penalty provisions under both section 1831 and section 1832 treat violations as a serious crime.¹⁰⁷ In addition, the territorial reach of the

owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly:

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information; knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in any of paragraphs (1) through (3); or (5) conspires with one or more persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

(b) Any organization that commits any offense described in subsection

(a) shall be fined not more than \$5,000,000.

18 U.S.C.A. § 1832 (West 1996).

¹⁰⁶ Pooley et al., *supra* note 46, at 193. The terms might also encompass some lawful business competitive intelligence practices. Pooley theorizes that the EEA may prohibit “reverse engineering”. *Id.* at 194. Reverse engineering involves obtaining a competitor’s product and disassembling the product to discover the properties and characteristics. *Id.* Individuals and corporations may become liable under the language in the act regarding “altering of a trade secret” or “sketching or drawing” of a product or process that qualifies as a trade secret. *Id.* However, the most common type of reverse engineering, looking at or testing of a lawfully obtained marketed commercial product to determine its content, will not be illegal under the EEA. *Id.* Furthermore, it is not likely that companies would choose to pursue a garden-variety action of reverse engineering for two reasons. First, almost all companies perform some type of reverse engineering. By fostering an environment of litigation, the company is itself potentially liable. Second, most companies would not prefer to generate animosity through litigation realizing that today’s competitors may become tomorrow’s partners.

¹⁰⁷ Section 1832 provides for up to a ten year imprisonment and an undetermined fine for individuals while permitting fines up to five million dollars for corporations and organizations. 18 U.S.C.A. § 1832 (West Supp. 1998). Furthermore, section 1831 provides heightened penalties for cases of foreign espionage by raising the maximum imprisonment to fifteen years and setting the maximum fine for organizations at ten million dollars. 18 U.S.C.A. § 1831 (West 1996). In addition, Section 1834 provides for the forfeiture of a defendant’s property during sentencing:

the court...shall order...that the person forfeit...any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as a result of such violation and...property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violation.

statute is extremely broad.¹⁰⁸ For these reasons, the EEA is the first federal criminal statute that has the potential to be an extremely potent method for deterring and punishing the theft of corporate trade secrets and proprietary business information.¹⁰⁹

However, a federal government approach under this statute is unlikely to protect the majority of businesses facing the rising problem of corporate espionage for four important reasons. First, the main target of this particular federal law is aimed at reducing the involvement of foreign countries in targeting U.S. industries in efforts to obtain their proprietary business information and trade secrets.¹¹⁰ Therefore, it is unlikely that the federal government will expend huge amounts of time,

18 U.S.C.A. § 1834 (West Supp. 1998).

¹⁰⁸ Pooley et.al., *supra* note 46, at 204. The act applies to activity conducted within the United States, but also to foreign activity, provided that any act "in furtherance of the offense was committed in the United States." *Id.* (quoting 18 U.S.C.A. § 1837). Considering that curbing foreign espionage was one primary goal behind the implementation of this law, a broad grant of jurisdictional power is needed to achieve that goal. Pooley et.al., *supra* note 46, at 204. The limitation of resources in terms of time and money combined with foreign policy considerations also inherently limits the government to prosecute only cases with a showing of considerable national interest. *Id.* See *infra* note 111.

¹⁰⁹ The strong points of this act are numerous. First, the EEA provides comprehensive scope and coverage through a broad definition of trade secret and confidential information. See *supra* notes 98-102. Second, the modes of theft and misappropriation covered are expansive and sweeping. See *supra* note 103. Third, the penalty provisions provide a powerful criminal deterrent. See *supra* note 107. Fourth, the EEA extends protection to theft and misappropriation by domestic and foreign instrumentalities. See *supra* note 108. This is a double-edged sword however, as the focus will primarily be on the illegal actions of foreign actors. See *infra* notes 109-111 and accompanying text. Upon signing the bill, President Clinton explained the overall significance of the EEA, "This act establishes a comprehensive and systematic approach to trade secret theft and economic espionage, facilitating investigations and prosecutions." Statement of the President of the United States, 1996 U.S.C.C.A.N. 4034 (Oct. 11, 1996). While the EEA was certainly an important first step in the addressing of this problem, the act will likely be more symbolic and figurative than used in prosecution by the U.S. government. See *infra* notes 110-20 and accompanying text.

¹¹⁰ One author states that the "[a]ct was passed primarily to 'level the playing field' in the international arena." Collins, *supra* note 34, at 15. The statute sends a clear and strong "hands off" signal to outside entities. *Id.* The legislative history strengthens this argument. "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." U.R. REP. NO. 104-788, at 7 (1996) ("The threat has become more diversified and complex."). Foreign intelligence services, both private and government sponsored are recognizing that national power is a function of economic power. *Id.* Because the United States is on the cutting edge of technological innovation, U.S. corporations are a prime target. See *supra* notes 15-16. While foreign economic espionage is a potentially massive problem that surely needs addressing, domestic espionage is as significant and potentially more dangerous to the U.S. economy.

effort, and money to investigate and prosecute domestic crimes and domestic criminal defendants.¹¹¹ Second, the FBI and federal government will focus their target most notably on wide spread, large-scale, egregious economic espionage where the evidence is clear and convincing.¹¹² This leaves a tremendous gap in cases where the espionage involves a relatively small activity in terms of monetary value and effort expended.¹¹³

Third, criminal law in general suffers inherently from four drawbacks that may decrease the motivation of corporations to enlist the help of the federal government.¹¹⁴ First, criminal statutes do not adequately protect the rights of the victim.¹¹⁵ Second, prosecutors do not have the expertise to prosecute high-tech crimes.¹¹⁶ Third, the victim relinquishes control of the case to the government.¹¹⁷ Fourth, the burden

¹¹¹ This may represent sentiments that foreign corporations and governments acting together create an unfair, and unrestricted power that U.S. corporations alone have difficulty counteracting. In comparison to other foreign powers, the U.S. government does not sponsor espionage activities. The federal government can remedy this inequity by using its resources to go after foreign entities more vigorously than domestic espionage. Furthermore, domestic espionage generally pits one equally matched company against another equally matched company on a familiar playing field. A dual approach may be the best way of combating the problem. The federal government pursues foreign players, while state criminal law attacks domestic theft and misappropriation. See *infra* Section III.

¹¹² Collins, *supra* note 110, at 14. The type of espionage the act was intended to thwart were clear cut cases with "smoking gun" evidence. *Id.* The government will pursue the fairly egregious cases rather than those "gray area" cases. *Id.* A number of factors delineate which cases are ripe for prosecution by the federal government: (1) whether the information was clearly a trade secret; (2) whether the information was technical or scientific in nature; (3) evidence of criminal intent and conduct; (4) evidence of the information's monetary value; (5) the availability of other remedies; (6) whether the misappropriation was promptly reported. Pooley et al., *supra* note 46, at 211. Two factors merit further brief discussion. As to number 6, the EEA fails to establish a statute of limitations. How quickly the matter was reported to the authorities is further complicated by the fact that many companies fail to discover the theft or are fearful of the consequences in reporting that theft. See *supra* note 38 and accompanying text. As to number 5, the focus of this Note theorizes that with powerful state law criminal approaches, the federal government will be able to effectively target the "featured" enemies. If state law adequately protects these rights, the federal government can invest more time and money in catching the "big-fish," notably foreign entities without the burden falling on smaller scale operations. See *supra* note 110.

¹¹³ The gap can be greatly closed by strong state criminal law. To date, state criminal law is out-dated and inadequate. See *infra* notes 163-195 and accompanying text.

¹¹⁴ Toren, *supra* note 15, at n.3.

¹¹⁵ *Id.*

¹¹⁶ *Id.*

¹¹⁷ *Id.*

of proof is higher in the criminal context than in civil litigation.¹¹⁸ A final weakness is that procedural difficulties accompany this statute for a period of time.¹¹⁹ Overlapping all of these weaknesses is the issue of whether the federal government will vigorously defend the rights of corporate America by enforcing the statute on the books.¹²⁰ For these reasons, state law will likely be the most effective avenue for a proactive deterrent approach to preventing the theft and misappropriation of trade secrets.

However, current state law is outdated, extremely narrow in scope, and lacks stiff penalty provisions. An investigation into the state law approaches will demonstrate that a new approach is necessary, using the Model Penal Code as its vehicle.

¹¹⁸ Band et al., *supra* note 23, at 1. The government has the burden of proving each element of the offense beyond a reasonable doubt. *Id.* The most difficult aspect will likely be proving the defendant had the criminal intent. *Id.* The government will likely prosecute cases where overwhelming evidence of criminal intent exists. *Id.* This coincides with the problems detailing the government's desire to prosecute egregious cases with "smoking gun" evidence. See *supra* note 112.

¹¹⁹ For example, when deciding which cases to prosecute, the decision requires the approval of numerous Justice Department officials all the way up the line to the Attorney General, Janet Reno. Band et al., *supra* note 23, at 1. This is troublesome in a few regards. First, the process is bound to get caught up in typical federal "red tape" which comes with agency action. *Id.* Second, when companies realize the potential uphill battle that will ensue just to investigative approval, most are likely to give up. *Id.*

¹²⁰ The prior federal statutes, such as mail and wire fraud were rarely enforced or prosecuted in the area of misappropriation and theft of trade secrets and business proprietary information. Band et al., *supra* note 23, at 1. Witnessed by the lack of enforcement based on prior statutory law, the concern remains whether federal words will speak louder than its actions. *Id.* Prosecutions may have been limited in the past primarily because inadequate statutes existed and awareness of the theft of this information has been only recently discovered to be a widespread problem. *Id.* Both play a role to some extent, but generally the federal government is less concerned with issues relating to white collar and business related crime. *Id.* It is unlikely that this statute will prompt the federal government to do an about face and to become involved in this area on a widespread basis. *Id.* Furthermore, as witnessed by the savings and loans scandals and insider trading debacle of the late 1980's, the federal government seems to address these issues in a reactive way, similar to civil litigation remedies. *Id.* As evidence of this reactive approach in the tree years since passage of the EEA, only one federal case has proceeded to trial. Daniel Eisenberg, *Eyeing the Competition*, TIME, March 22, 1999, at 59. As Eisenberg states discussing the impact of the EEA, "the good guys haven't had much luck yet." *Id.* at 58. While the FBI has expended more effort and resources to investigate corporate espionage, the EEA's success in terms of prosecutions and convictions remains negligible. *Id.*

III. STATE CRIMINAL LAW APPROACHES TO THE THEFT AND
MISAPPROPRIATION OF TRADE SECRETS AND PROPRIETARY BUSINESS
INFORMATION

A. Introduction

Both federal statutory law and state statutory law play important roles in formulating an effective criminal deterrent to the theft and misappropriation of trade secrets and confidential commercial information.¹²¹ While federal legislation only recently followed the trend of implementing a more comprehensive protection of valuable commercial information with the passage of the EEA,¹²² state criminal law has protected trade secrets since the late 1960s.¹²³ However, only

¹²¹ Eli Lederman, *Criminal Liability for Breach of Confidential Commercial Information*, 38 EMORY L.J. 921 (1989). As witnessed by *supra* notes 88-93 and accompanying text, current federal criminal law leaves large gaps in the protection of trade secrets and proprietary business information. While the EEA remedies numerous limitations of prior federal law, the EEA, as discussed in *supra* notes 110-120 and accompanying text, provides a federal legislative approach to an inherent state law issue. Corporations and businesses are governed by the laws of the state in which they incorporate. WILLIAM L. CARY & MELVIN A. EISENBERG, *CORPORATIONS* 125 (7th ed. 1995). Furthermore, the American general business climate tends to prefer a federalistic theory of economic regulation, feeling more comfortable with state supervision and control as opposed to federal government interference in corporate affairs. Management of both small privately held corporations and large publicly held corporations are more likely to report theft and misappropriation of trade secrets to local authorities, as opposed to reporting to the federal government for prosecution. See *supra* note 112. With local authorities, the company has a greater ability to retain some control over the investigation and prosecution. Furthermore, companies have a much easier procedural route to obtaining quick and effective prosecution using local authorities and state law. See *supra* note 119. However, current state law in almost every state fails to adequately protect corporations. See *infra* notes 163-195 and accompanying text. With companies reluctant to utilize the current federal criminal law approach, state law needs to furnish the companies with an effective alternative prosecution vehicle. See *infra* Section IV.

¹²² See *supra* notes 98-120. Also, only recently did the federal judiciary contribute to expanded scope by broadly construing federal statutory schemes. *Carpenter*, 484 U.S. at 19. However, as illustrated the federal judiciary has limited the scope of protection by narrowly construing other federal statutes. *Brown*, 925 F.2d at 1307. The patchwork nature of federal legislation was rectified by passage of the EEA. See *supra* notes 98-120. However, the EEA also fails to adequately protect businesses from the theft and misappropriation of trade secrets and proprietary business information. See *supra* notes 110-120.

¹²³ Lederman, *supra* note 121, at 935. The state law trend can be described in three stages. In the 1960's both civil and criminal trade secret statutes were passed establishing protection of commercial information for the first time. *Id.* at 997. The 1970's witnessed a growth in the passage of computer related trade secret criminal laws. *Id.* These statutes explicitly covered information residing in computers. *Id.* See, e.g., CAL. PENAL CODE § 502 (West 1988); DEL. CODE ANN. tit. 11, §§ 931-939 (1987); IND. CODE ANN. §§ 35-43-1-4, 35-43-2-3 (Burns Supp. 1989); MICH. COMP. LAWS ANN. §§ 751.797-752.791 (West Supp. 1989);

thirty states currently have criminal laws addressing the theft and misappropriation of trade secrets and confidential business information¹²⁴ and the statutes vary widely as to scope, coverage and prohibited modes of transfer.¹²⁵ Before discussing the various state approaches, it is useful to illustrate the aspects where the majority of the states have found common ground.

State criminal statutory law converges with regard to two "fixed" elements or prerequisites.¹²⁶ First, almost all of the statutes dealing with

N.Y. PENAL LAW §§ 156.00-156.50 (McKinney 1998); TEX. PENAL CODE ANN. §§ 33.01-33.05 (Vernon 1989). The 1980's witnessed an expansion of trade secret protection through broad interpretations of the various federal statutes, including the federal mail and wire fraud statutes. Lederman, *supra* note 121, at 997-98. However, the judiciary also significantly narrowed the scope of the ITSA. See *supra* notes 61-69. Furthermore, protection is limited by the requirements of the statute. See *supra* notes 89-91 and accompanying text. The development of state criminal law in the past 20 years has not kept pace with the widespread use and importance of trade secret and confidential information. The outdated criminal, unfortunately, coincides with the ease and powerful incentive to steal trade secrets and confidential information. S. REP. NO. 104-359, at 6-7 (1996). Over the past twenty years, the majority of states have adopted civil remedies but only a few states have adopted, modified, or updated new criminal statutes dealing explicitly with the theft of trade secrets. *Id.* See *infra* notes 163-195. In addition, most state laws in this area punish only by misdemeanors and are rarely used by prosecutors. *Id.* See *infra* note 194.

¹²⁴ Twelve states have promulgated specific statutes directly covering the theft of trade secrets. ALA. CODE § 13A-8-10.4 (1994); ARK. CODE ANN. § 5-36-107 (Michie 1997); CAL. PENAL CODE § 499C (West Supp. 1999); COLO. REV. STAT. ANN. § 18-4-408 (West 1990); FLA. STAT. ANN. § 812.081 (West Supp. 1999); GA. CODE ANN. § 16-8-13 (1996); OKLA. STAT. ANN. tit. 21, § 1732 (West Supp. 1999); 18 PA. CONS. STAT. ANN. § 3930 (West Supp. 1998); S.C. CODE ANN. § 39-8-90 (Law Co-op. Supp. 1997); TENN. CODE ANN. § 39-14-138 (1997); TEX. PENAL CODE ANN. § 31.05 (West 1994); WIS. STAT. ANN. § 943.205 (West Supp. 1998). 13 states take the approach of including the theft of trade secrets under criminal statutes relating to crimes against property. CONN. GEN. STAT. ANN. § 53a-124 (West 1994); DEL. CODE ANN. tit. 11, § 857 (1995); IDAHO CODE § 18-2402 (1997); 72 ILL. COMP. STAT. ANN. 5/15-8 (West 1993); IND. CODE ANN. § 35-41-1-23(a)(9) (West 1998); ME. REV. STAT. ANN. tit. 17A, § 352(1)(F) (West 1983); MD. CODE ANN. CRIM. LAW § 340(h)(11) (1992); MINN. STAT. ANN. § 609.52(1) (West Supp. 1999); N.C. GEN. STAT. § 14-75-1 (1997); N.H. REV. STAT. ANN. § 637:2(I) (1986); N.J. STAT. ANN. § 2C:20-1 (West Supp. 1998); OHIO REV. CODE ANN. § 2901.01 (Anderson 1997) UTAH CODE ANN. § 76-6-401 (1995). Two states include trade secret protection under larceny statutes. MASS. GEN. ANN. LAWS ch. 266 § 30 (West Supp. 1998); N.Y. PENAL LAW §§ 155.00, 155.30, 165.07 (McKinney 1979). Finally three states address the matter via protection under statutes for computer crimes. LA. REV. STAT. ANN. §§ 14:73.1-2 (West 1997); MISS. CODE ANN. §§ 97-45-1-11 (1994); WYO. STAT. ANN. §§ 6-3-501, 3-502 (Michie 1997). This leaves 24 states with absolutely no statutory protection under current law.

¹²⁵ See *infra* notes 164-175 and accompanying text.

¹²⁶ Lederman, *supra* note 121, at 943. Secrecy and economic value "constitute the prerequisites that delineate the boundaries of...confidential commercial information protection." *Id.* at 936. Once inside those boundaries, however, each state takes a different approach. See *infra* notes 127-131 and accompanying text.

the theft of trade secrets and confidential business information require the preservation of secrecy as a prerequisite for qualification under the statute.¹²⁷ A second prerequisite exists as to the issue of economic value of the information or trade secret.¹²⁸ The two prerequisites, secrecy and

¹²⁷ Lederman, *supra* note 121, at 938. Most of the statutes determine the conditions for the establishment of secrecy status. *Id.* Many states require that the steps and effort the possessor takes to protect the information be "reasonable under the circumstances." DEL. CODE ANN. tit. 6, § 2001(4)(b) (Supp. 1988); MINN. STAT. ANN. § 609.52 (1) (6)(ii) (West Supp. 1999); OKLA. STAT. ANN. tit. 21 § 1732 (West Supp. 1999); WIS. STAT. ANN. §§ 134.90(1)(c) (2), 943.205(2)(e) (West 1982 & Supp. 1989). Courts have interpreted these statutes to require that the possessor of the trade secret exercise active or affirmative measures to guard the information's confidentiality. *See, e.g.,* Amoco Prod. Co. v. Lindley, 609 P.2d 733, 743 (Okla. 1980). Other states require specific proof that the information is secret. Tennessee allows the information to qualify as a trade secret only when, "the owner takes measures to prevent it from becoming available to persons other than those selected by the owner." TENN. CODE ANN. § 39-14-138 (1997). *See also* CAL. PENAL CODE § 499C (West Supp. 1999); N.J. STAT. ANN. § 2C:20 (West Supp. 1998). Many states have defined secrecy and implemented tests. Once the possessor meets the requirements of the test, the information is presumed to be a secret. For example, secrecy under Pennsylvania law requires that the owner identifies the information as confidential and that the information has not been published or become a matter of general public interest. 18 PA. CONS. STAT. ANN. § 3930 (West Supp. 1998). After meeting this threshold test, Pennsylvania law states, "There shall be a rebuttable presumption that scientific, technical...or confidential information that has not been published or otherwise become a matter of general public knowledge qualifies as a trade secret." *Id.* *See also* COLO. REV. STAT. ANN. § 18-4-408 (West 1990); MISS. CODE ANN. §§ 97-45-1-11 (1994). While the language differs from state to state, a keystone requirement throughout all of the states is that the information remains confidential or secret. Lederman, *supra* note 121, at 938. The only exception to this requirement occurs in Massachusetts. The Massachusetts statutory approach to protection of trade secrets is covered under theft of property, and property is defined to include both tangible and intangible objects. MASS. GEN. ANN. LAWS ch. 266 § 30 (West Supp. 1998). The Massachusetts language posits no requirement that the object remain confidential, or obtain secrecy status to qualify for protection under the statute. *Id.*

¹²⁸ Some states express this in terms that are extremely simplistic, the trade secret or confidential information must be of "value" or "valuable." ARK. CODE ANN. § 5-36-107 (Michie 1997); COLO. REV. STAT. ANN. § 18-4-408 (West 1990). Other states define property as "anything of value" and explicitly include trade secrets in the definition. The language from Indiana is representative of this approach, "Property means anything of value. The term includes: trade secrets, intangibles, real property, personal property, money, labor and services." IND. CODE ANN. § 35-41-1-23(a)(9) (West 1998). *See also* MD. CODE ANN. CRIM. LAW § 340(h)(11) (1992); UTAH CODE ANN. § 76-6-401 (1995). Others follow the UTSA definition that the "information must derive independent economic value, actual or potential, from not being generally known to and not being readily ascertainable by proper means." *See, e.g.,* DEL. CODE ANN. tit. 11, § 857 (1995); MINN. STAT. ANN. § 609.52(1) (West Supp. 1999); WIS. STAT. ANN. § 943.205 (West Supp. 1998). Others have referred to the concept that the trade secret must facilitate the gaining of competitive advantage. For instance, Florida statutory language requires the information to be "of advantage to the business, or providing an opportunity to obtain an advantage over those who do not know or use it when the owner takes measures to prevent it from becoming available to persons other than those selected by the owner." FLA. STAT. ANN. § 812.081 (West Supp. 1999).

economic value, are closely connected.¹²⁹ Secrecy endows the information with independent economic value.¹³⁰ Conversely, having an independent economic value justifies the protection of the information under the statutes.¹³¹

However, state criminal statutory law widely diverges as to the variable elements including scope, coverage and prohibited modes of transfer.¹³² Part B of this Section will provide an overview of state criminal law approaches by grouping individual states into representative models based on these variable elements.¹³³ The overview and discussion will provide a useful means for comparison between the states and create a framework for part C of this Section, which will detail

Regardless of the terminology, the key issue is that the majority of the statutes posit a requirement that the possessor affirmatively prove that the confidential information or trade secret maintains some minimal level of economic value, whether it be real or potential, present or in the future. Lederman, *supra* note 121, at 936. Only Massachusetts abrogates this requirement. See MASS. GEN. ANN. LAWS ch. 266 § 30 (West Supp. 1998).

¹²⁹ Lederman, *supra* note 121, at 936.

¹³⁰ *Id.*

¹³¹ *Id.*

¹³² Lederman, *supra* note 121, at 943. The variable elements (namely the information content and proscribed modes of transfer) are critical to an effective analysis of current state law approaches. *Id.* First, these elements shape the exact extent of the protection under the law. *Id.* Second, they tend to dominate the subject matter's trend of development. *Id.* Generally the content element consists of two groups of situations. *Id.* The deliberate and restrained group limits the protection to scientific and technical information. *Id.* at 943-44. The second group gradually extends the boundaries to encompass other forms of confidential business information. *Id.* at 944. The element regarding prohibited modes of transfer is categorized into four sets. *Id.*

[1] [P]rohibited modes...[are] limited solely to unauthorized corporeal (physical, material) acquisition...[with] the information being...undetached from the physical article containing it, [2] [E]ncompasses, apart from corporeal acquisition, corporeal transmission and transformation of information from one tangible container or source to another....[3] The other group...include[s]...the two modes of corporeal transfer, incorporeal transmission or transformation...[4] [R]etention of information in a totally incorporeal (non-physical, non-material) mode.

Id. at 944.

After detailing two sets of content classifications and four sets of mode categorizations, Lederman develops as the thesis for his Article, eight models that all states fall into. *Id.* at 945. However, my analysis will be less detailed and the states will be grouped into four representative "models."

¹³³ See *infra* notes 135-162

the limitations and problems presented by the current state criminal law approaches.¹³⁴

B. Overview of State Criminal Law Trade Secret Laws

Five state criminal statutes limit the prohibited mode of transfer to strictly corporeal acquisition of the physical, tangible article containing the trade secret.¹³⁵ For example, Illinois characterizes theft as "obtaining or exerting control over property of the owner" and limits that phrase to physically "taking, carrying away, or conveying of possession of property."¹³⁶ Two of these states further erode trade secret protection by limiting the scope of coverage to strictly scientific and technical material.¹³⁷ The other three states include within their trade secret definition a more expansive scope including additional types of commercial information.¹³⁸

Another cluster of states have strictly limited the content of protection to include only scientific and technical information.¹³⁹

¹³⁴ See *infra* notes 163-195.

¹³⁵ These statutes generally encompass activities that fall under traditional theft offenses. Lederman, *supra* note 121, at 948. Therefore, none of these five states directly protect trade secrets. *Id.* The statutes are drafted to protect property rights, and each state has defined property differently. *Id.* See *infra* notes 136-138 and accompanying text.

¹³⁶ 720 ILL. COMP. STAT. ANN. 5/15-8 (West 1993). Maryland characterizes theft in an identical manner, limiting the phrase "exerts control" to acts involving property which "bring about a transfer of interest or possession, whether to the offender, or to another." MD. CODE ANN. CRIM. LAW § 340(g)(1) (1992). See also CONN. GEN. STAT. ANN. § 53a-124 (West 1996); IDAHO CODE § 18-2402 (1997); N.C. GEN. STAT. § 14-75.1 (1997).

¹³⁷ For example, Connecticut limits the material covered to "a sample, culture, specimen....record, recording or document...which constitutes or reflects a secret scientific or technical process, invention, or formula." CONN. GEN. STAT. ANN. § 53a-124 (West 1994). The language of the North Carolina statute is nearly identical to the Connecticut version. See N.C. GEN. STAT. § 14-75.1 (1997).

¹³⁸ The other three states that fall under this model offer a more broad definition of property. Maryland is representative of this approach and in addition to protecting scientific information also includes under the definition of property "blueprints, financial instruments and information, management information, merchandising and design processes, and formulas." MD. CODE ANN. CRIM. LAW § 340(i)(12) (1992). Both Idaho and Illinois define property in a manner almost identical to the Maryland approach. See IDAHO CODE § 18-2402 (1997); 720 ILL. COMP. STAT. ANN. 5/15-1 (West 1993).

¹³⁹ New York, for example, proscribes only the theft of "secret scientific information". N.Y. PENAL LAW §§ 155.00, 155.30, 165.07 (McKinney 1997). However, the language is somewhat more expansive than covering purely scientific matters, but also includes records of a technical process, invention or formula. However, the language is in a purely scientific context, limiting its application to purely business information. Other statutes suffer from the same problems. Georgia and Tennessee have defined trade secrets to include "the whole or any portion or phase of scientific or technical information, design,

However, these state statutes have broadened the proscribed modes of transfer.¹⁴⁰ The statutes provide greater protection by proscribing unauthorized reproduction of a trade secret, but only to the extent that the reproduction is embodied in a tangible item.¹⁴¹

The next wave of states provide an enhanced definition of the term trade secret increasing the scope of coverage, while maintaining the expanded list of proscribed modes of transfer.¹⁴² In addition to

process, procedure, formula, or improvement which is secret and of value." GA. CODE ANN. § 16-8-13(a)(4) (1996); TENN. CODE ANN. § 39-14-138(a)(4)(1997). The statutes recognize trade secrets, but suffer huge drawbacks because they narrowly define the terms, limiting protection to only scientific or technical matters or information. These statutes would not apply to the majority of business, financial, economic, marketing, or production information. For companies focusing their products and services on scientific information, such as pharmaceutical companies or bio-technology companies, these statutes would likely cover much of their confidential information. However, for companies manufacturing automobiles or computers or providing banking or financial services, these statutes would be absolutely worthless.

¹⁴⁰ New York prohibits the theft appropriation of tangible, physical substances, while also expanding the proscribed mode of transfer to include the unauthorized making of "a tangible reproduction or representation of such secret...material by means of writing, photographing, drawing, mechanically or electronically reproducing or recording..." N.Y. PENAL LAW § 165.07 (McKinney 1999). In protecting the underlying information, this statute constitutes the first step forward in protecting purely intangible information. Georgia and Tennessee address this by proscribing copying of the article representing the trade secret and defining the term "copy" to include "any facsimile, replica, photograph, or other reproduction...and any note, drawing or sketch." GA. CODE ANN. § 16-8-13 (1996); TENN. CODE ANN. § 39-14-138 (1997).

¹⁴¹ This solves the problem of the thief copying or transferring the information to another tangible object and stealing only that object. However, these statutes would fail to extend criminal penalties to a theft which occurs by memorization of the information for future use or disclosure. Lederman, *supra* note 121, at 953. As long as a lapse of time exists between the memorization of the original confidential material and its subsequent reproduction or disclosure, no criminal liability arises. *Id.* The model followed by these states prohibits only "tangible reproductions or representations" of the information or material. *Id.* This model is a step forward from the previous statutes, but still fails to cover all of the potential modes of transfer. See *supra* notes 135-136.

¹⁴² These states include other forms of confidential information while prohibiting the unauthorized transmission and acquisition of tangible articles representing trade secrets. Lederman, *supra* note 121, at 954. For example, Florida proscribes theft or embezzlement of a trade secret and theft and embezzlement of an article "representing" a trade secret. FLA. STAT. ANN. § 812.081 (West Supp. 1999). Furthermore, Florida imposes criminal liability on one "who causes to be made a copy of an article representing a trade secret." *Id.* Florida defines the term copy as "any facsimile, replica, photograph or other reproduction..." *Id.* Minnesota and Oklahoma sanction the copying of trade secrets and the unlawful "representation of trade secrets." MINN. STAT. ANN. § 609.52(1) (West Supp. 1999); OKLA. STAT. ANN. tit. 21, § 1732 (West Supp. 1999). Both statutes define representation to include "depicting, recording, embodying, containing and constituting."

protecting scientific and technical information, these state statutes provide a definition of trade secrets that encompasses more general business or commercial information.¹⁴³ While these statutes correctly expand both content coverage and incorporate more modes of transfer, the statutes still fail to cover the transmission of trade secrets or business information via purely intangible means.¹⁴⁴

The next significant move involves proscribing modes of transfer apart from physical stealing and unlawfully duplicating the article in a tangible medium.¹⁴⁵ These statutes reach the incorporeal transmission of trade secrets such as unauthorized disclosure, exposure, or communication to another.¹⁴⁶ These models emphasize the abstract nature of the protected substance, but also recognize that economic value

Id. These statutes gradually expand the modes of transfer to encompass reproduction of trade secrets beyond mere copying or photographing. *Id.*

¹⁴³ Lederman, *supra* note 121, at 955. These states include other forms of confidential information while prohibiting the unauthorized transmission and acquisition of tangible articles representing trade secrets. *Id.* at 954. Florida, Minnesota and Oklahoma represent this approach. Florida defines trade secrets to include, "any compilation of information which ... is used in the operation of a business ... including any list of suppliers, list of customers, or business code." FLA. STAT. ANN. § 812.081(1)(c) (West Supp. 1999). Minnesota and Oklahoma expand trade secret status to "information, compilations, method, technique, or process ... that derives independent economic value, actual or potential from not being generally known." MINN. STAT. ANN. § 609.52(6)(i) (West Supp. 1999); OKLA. STAT. ANN. tit. 21, § 1732 (West Supp. 1999). The language of these statutes expands coverage by defining trade secret in a broad manner. No specific category of information is covered so long as the company can show the information meets the prerequisites of secrecy and independent economic value, the information qualifies under the language of these statutes. *Id.* See *supra* notes 127-31.

¹⁴⁴ The states that follow this model maintain the structural aspects evidenced by other models. Lederman, *supra* note 121, at 953. This model prohibits the unauthorized corporeal acquisition of the actual confidential information and any article which represents the trade secret. *Id.* Furthermore, this model continues to sanction unpermitted transmission of the information through copying and representing the information in any tangible object. *Id.* However, these statutes do not completely cover the theft of trade secrets. See *infra* notes 145-148 and accompanying text.

¹⁴⁵ Lederman, *supra* note 121, at 955.

¹⁴⁶ Lederman, *supra* note 121, at 955. Pennsylvania proscribes not only reproducing the trade secret but also the "exhibition of such article to another." 18 PA CONS. STAT. ANN. § 3930 (West Supp. 1998). The prohibited modes of transfer in Wisconsin are extremely similar. Wisconsin prohibits the exhibition, disclosure, and description of the secret information. WIS. STAT. ANN. § 943.205 (West Supp. 1998). The importance of the language under these statutes is that it extends prosecution to cases of breach of confidence by a person to whom the trade secret was entrusted. Lederman, *supra* note 121, at 955-56. However, the statutory language conditions criminal liability upon the performance of an overt act. *Id.* at 956. The thief must exhibit some physical manifestation such as communicating, disclosing, or unlawfully viewing the confidential information. *Id.*

can be lost or diminished without actually damaging the physical article.¹⁴⁷ A group of states has taken this proposition further and explicitly and unequivocally recognized the theft of information in a purely intangible form.¹⁴⁸

These states address not only the incorporeal disclosure and communication, but also incorporeal retention, memorization, and visual retention of trade secrets.¹⁴⁹ These statutes contain virtually no restrictions regarding the banned modes of transferring confidential business information and trade secrets.¹⁵⁰ The limitation in these statutes concerns the content of the protected information.¹⁵¹ These statutes

¹⁴⁷ Lederman, *supra* note 121, at 957. Prior statutes that prohibited copying or reproduction of the trade secret in a separate object symbolized the traditional idea of tangible deprivation. *Id.* However, these statutes recognize the impairment to the owner of the trade secret or confidential information by unauthorized communication or disclosure produces as much damage as a tangible deprivation. *Id.* The rationale and perception of these statutes represents an extremely important development in the criminal law regarding theft of trade secrets. *Id.* The prohibition against unauthorized exhibition, disclosure and communication of a trade secret completely disconnects the causation of damage from the tangible deprivation of the article. *Id.* at 957. These states clearly recognize that the damage accompanied by disclosure of the secret information to the detriment of the owner and the consequential harm suffered from is more than mere theft of a physical object. *Id.*

¹⁴⁸ In addition to forbidding the unauthorized communication or transmission of a trade secret, or copying the article representing the trade secret, Alabama and Texas have included a general prohibition against stealing trade secrets by any means. ALA. CODE § 13A-8-10.4 (1994); TEX. PENAL CODE ANN. § 31.05 (West 1994). These provisions encompass the physically carrying away of an article containing confidential information. *Id.* Furthermore, the statutory language in these states is broad enough to explicitly and unequivocally recognize theft of information through incorporeal retention, namely the intentional unauthorized acquisition by listening or viewing of the information and subsequent memorization. Lederman, *supra* note 121, at 958.

¹⁴⁹ These statutes define the trade secret itself as the object of the theft. Lederman, *supra* note 121, at 958. For example Texas defines stealing as "acquiring property by theft." TEX. PENAL CODE ANN. § 31.05 (West 1994). Property, under the Texas statutes, includes any tangible or intangible substance. *Id.* According to the Texas statute, one can steal information in its intangible form, detached from the physical article containing it. *Id.* See also Lederman, *supra* note 121, at 958. Statutory language in other states prohibits the exercise of "unauthorized control" over trade secrets, with control construed to extend beyond traditional modes of theft or larceny. See ME. REV. STAT. ANN. tit. 17A, § 352(1)(F) (West 1983); N.H. REV. STAT. ANN. § 637:2(J) (1986); UTAH CODE ANN. § 76-6-401(i) (1995).

¹⁵⁰ Lederman, *supra* note 121, at 961. Under this approach, the theft of information can occur without an overt act, namely without leaving a "clear mark on reality," even to the extent that the information holder is not aware of the offense. *Id.* From a practical perspective, however, the commission of the crime will not be uncovered unless the thief (after obtaining the information by listening, peeping, or memorizing) performs an overt act such as selling or communicating the information. *Id.*

¹⁵¹ Lederman, *supra* note 121, at 961.

narrowly define trade secrets, rarely covering any confidential business or commercial information.¹⁵² Thus, only three states have criminal trade secret statutes that adequately protect the interest of the trade secret possessor.¹⁵³

Colorado and Massachusetts have augmented protection by combining the growth trends through expanding the scope of the content protected under a definition of trade secrets¹⁵⁴ while proscribing the entire range and assortment of modes of transferring information.¹⁵⁵ Furthermore, Delaware's combination of an expansive list of prohibited

¹⁵² Texas for example defines trade secrets as, "any scientific or technical information design, process, procedure, formula, or improvement." TEX. PENAL CODE ANN. § 31.05(a)(4) (West 1994). Alabama and Utah define trade secrets in a verbatim manner. ALA. CODE § 13A-8-10.4(a)(4) (1994); UTAH CODE ANN. § 76-6-401(i) (1995).

¹⁵³ These states, of course, do not represent the business centers of America, like New York, Los Angeles, or Chicago. The statutes in these three states are extremely comprehensive and highly functional and while they protect companies within their states well, the use for "foreign" business is inherently limited.

¹⁵⁴ The confidential information in terms of content, embodies the various type of information commonly used in commerce and industry. Lederman, *supra* note 121, at 962. Colorado defines trade secrets as follows, "any scientific or technical information, design, process, procedure or formula, improvement, confidential business, or financial information...or other information relating to any business or profession." COLO. REV. STAT. § 18-4-408(d) (West 1990). Massachusetts defines trade secrets to include "anything tangible or intangible which represents secret merchandising, production or management information, design, process, procedure or improvement. MASS. GEN. ANN. LAWS ch. 266 § 30 (West Supp. 1998). Both statutes explicitly refer to secret business and commercial information. *Id.*

¹⁵⁵ The statutes cover all four modes: corporeal acquisition, incorporeal transmission through disclosure, incorporeal retention of information in an intangible state, and copying or reproducing the secret information to a separate tangible article. The Colorado statute reads in pertinent part:

(1) Any person who, with the intent to deprive or withhold from the owner thereof the control of a trade secret, or with the intent to appropriate a trade secret to his own use or to the use of another, steals, or discloses to an unauthorized person a trade secret, or, without authority, makes or causes to be made a copy of an article representing a trade secret, commits theft of a trade secret

(a) "article" means any object, material, device, or substance, or copy thereof, including any writing, record, recording, drawing, sample, specimen, prototype, model, photograph, microorganism, blueprint, or map

(b) "copy" means any facsimile, replica, photograph, or other reproduction of an article, and any note, drawing, sketch made of or from an article

(c) "representing" means describing, depicting, containing, constituting, reflecting, or recording.

COLO. REV. STAT. § 18-4-408 (West 1990).

modes of transfer, together with a sweeping list of protected property, places it at the extensive end of the spectrum of comprehensive protection of trade secrets and confidential business information through state criminal law.¹⁵⁶

Delaware has produced a criminal trade secret statute that protects all confidential proprietary information by broadly defining the term "trade secret."¹⁵⁷ Delaware statutory language also encompasses all four modes of theft and transmission of trade secrets and confidential business information.¹⁵⁸ First, Delaware prohibits unauthorized corporeal transmission or acquisition of tangible articles containing the trade secret or confidential information.¹⁵⁹ Second, Delaware prohibits the unauthorized copying or reproduction of the trade secret or confidential information in a separate tangible article.¹⁶⁰ Third,

¹⁵⁶ Lederman, *supra* note 121, at 964. The Delaware statutory approach is similar to Colorado and Massachusetts, although the Delaware approach is of much more practical importance to many American corporations. Over 40% of the firms listed on the New York Stock Exchange (NYSE) are incorporated in Delaware. CARY & EISENBERG, *supra* note 121, at 126. Both the statutory and common law of Delaware are aimed at attracting businesses to incorporate in their state. *Id.* Providing "pro-business" statutory trade secret protection may facilitate business incorporation within the state. It is no coincidence that Delaware has the best statute on the books.

¹⁵⁷ Lederman, *supra* note 121, at 964. Delaware language is read to cover any and all confidential information of economic value and reads in pertinent part:

(4) Trade Secret shall mean information, including a formula, pattern, compilation, program, device, method, technique or process, that:

(a) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and

(b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

DEL. CODE ANN. tit. 6 § 2001 (1995).

The broad Delaware language encompasses and protects all proprietary, confidential information by including the information under the definition of trade secret. Also, the statute poses no structural limitations by never including any term or phrase regarding "scientific or technical information." Furthermore, the Delaware statute broadly defines theft to include all three modes of transmission. *See infra* notes 158-162 and accompanying text.

¹⁵⁸ DEL. CODE ANN. tit. 11 § 857 (1995).

¹⁵⁹ Theft is defined to include the physical deprivation or withholding of trade secrets by another person permanently or for an extended period of time. DEL. CODE ANN. tit. 11 § 857 (1995).

¹⁶⁰ Any means of obtaining or exercising control over the trade secret, regardless of whether the theft involved the original tangible object containing the trade secret or the theft involved a separate article embodying the trade secret will trigger the statute. DEL. CODE ANN. tit. 11 § 857 (1995).

Delaware prohibits the incorporeal transmission and acquisition of trade secrets and confidential information through unauthorized exposure, disclosure and communication.¹⁶¹ Finally, Delaware recognizes theft of trade secrets and confidential information in a purely intangible manner by prohibiting transmission and acquisition through incorporeal retention and memorization.¹⁶² Currently, only these three states afford an adequate criminal law deterrent to the theft of trade secrets and proprietary business information.

C. *Limitations of Current State Criminal Law Approaches*

An evaluation of the remaining twenty-seven state law approaches to the protection of trade secrets and proprietary business information through criminal law reveals numerous practical weaknesses.¹⁶³ First, the majority of states lack an adequate definition of information qualifying for protection as a trade secret or confidential business information.¹⁶⁴ The language in sixteen of the twenty-seven state statutes explicitly confines itself to scientific or technical information.¹⁶⁵ The language of these sixteen state statutes never directly or explicitly covers confidential commercial, economic, or business information.¹⁶⁶ This lack of breadth and depth in the definition and protection of trade secrets leads to serious problems.¹⁶⁷ In contrast, the EEA includes

¹⁶¹ Misappropriation is defined broadly to include any "acquisition of a trade secret by improper means or disclosure or use of a trade secret without the consent of the owner." DEL. CODE ANN. tit. 11 § 857 (1995). Acquisition can be in the form of exposure, disclosure, or communication of the trade secret. *Id.*

¹⁶² The statute forbids the exercise of any unpermitted control, including incorporeal retention over any type of economically valuable intangible confidential information. DEL. CODE ANN. tit. 11 § 857 (1995).

¹⁶³ See *infra* notes 164-195 and accompanying text.

¹⁶⁴ Lederman, *supra* note 121, at 947-48.

¹⁶⁵ *Id.* at 952-3. See *supra* notes 137, 139, 151-52 and accompanying text.

¹⁶⁶ Lederman, *supra* note 121, at 952-53. A reading of the language of these statutes clearly leads to the conclusion that the statute imposes criminal liability upon the theft of one specific type of information, unrelated to any business related field. *Id.* The only theft triggering these statutes involves stealing scientific or technical trade secrets or confidential information. *Id.*

¹⁶⁷ The applicability of these statutes is extremely limited to the majority of companies and businesses operating in the United States currently. Most notably the language would not cover the operations of accounting firms, banks, insurance companies, and most consumer goods manufacturers. Under the majority of state statutes, any document related to the day to day operations or future strategic plans of a business enterprise would not be covered. For example, confidential financial data, customer and supplier lists, and marketing plans do not fall under any category of scientific or technical information. See *supra* notes 139 and 152 and accompanying text.

confidential commercial, economic and business information in its definition of a trade secret.¹⁶⁸

The distinction between commercial, business information and scientific, technical information is delineated in almost all of the statutes.¹⁶⁹ As one scholar explains, "this distinction was based on the assumption that...scientific information usually constitute[s]...a clearer creative investment, deserving broader protection due to functional and value considerations."¹⁷⁰ This distinction is clearly outdated and based on faulty assumptions, as business and commercial information along with financial data represent innovation, value and usefulness in the same regard as scientific discovery, only in a different context.¹⁷¹ Another justification for the distinction was that theft of scientific information was easier to prove than certain types of commercial information.¹⁷² This distinction may have some merit.¹⁷³ Although, with the increasing value of proprietary business information, corporations will have tighter methods of protection, allowing for easier proof of theft.¹⁷⁴ The limited and narrow definition of trade secrets under a majority of state criminal law statutes prevents those statutes from producing an adequate criminal deterrent.¹⁷⁵

Second, most state statutes fail to proscribe many forms or modes of transmission.¹⁷⁶ Currently, of the thirty states with criminal statutory protection for trade secrets, over one-half strictly limit the proscribed modes of theft to corporeal acquisition and transmission.¹⁷⁷ Corporeal acquisition is limited to the physical carrying away of the actual item that contains the trade secret.¹⁷⁸ Corporeal transmission would include copying or reproducing the secret information in a tangible object separate from its original form and physically carrying away that

¹⁶⁸ See *supra* notes 98-102.

¹⁶⁹ Lederman, *supra* note 121, at 962.

¹⁷⁰ *Id.*

¹⁷¹ It's hard to argue that developing a scientific process that allows plants to grow at twice the rate of speed deserves more protection than the invention a manufacturing process, (such as the assembly line at Ford) or marketing plan, such as the Nike "Just Do It."

¹⁷² Lederman, *supra* note 121, at 962.

¹⁷³ *Id.*

¹⁷⁴ *Id.*

¹⁷⁵ *Id.* at 947. The language of these statutes is clearly designed to cover and protect scientific and technical information only.

¹⁷⁶ *Id.*

¹⁷⁷ *Id.*

¹⁷⁸ Lederman, *supra* note 121, at 948.

separate object.¹⁷⁹ The primary purpose of these statutes is not to protect the value of the information contained in the object, but to protect the physical article or object itself from theft.¹⁸⁰ These statutes are designed to maintain a physical, unbroken link between the information and the physical object.¹⁸¹ For criminal liability to attach, the thief must physically steal the original tangible object containing the trade secret or a separate tangible object representing or embodying the trade secret.¹⁸² However, if the theft occurs through incorporeal transmission or retention, such as memorization and subsequent disclosure, communication, or exhibition, criminal liability would not attach.¹⁸³ Furthermore, any theft by intangible means, such as transferring the data by computer, would not trigger any criminal liability.¹⁸⁴ In contrast, the EEA approach covers all four modes of acquisition and transmission.¹⁸⁵ These first two weaknesses of state law can be explained by the time period in which they were drafted.¹⁸⁶ The approaches promulgated by the states were adequate twenty years ago, but are outdated and deficient in today's global economy.¹⁸⁷

¹⁷⁹ *Id.* at 950-4.

¹⁸⁰ *Id.* at 947.

¹⁸¹ *Id.*

¹⁸² *Id.*

¹⁸³ *Id.* See *supra* notes 146-150. For example, an athletic apparel company may want to produce a secret television marketing plan or strategy. The company designs and reproduces the plan on a series of tangible objects or articles. If the thief views the plan and communicated the information to a competitor, no criminal liability would accrue. For criminal liability to accrue, the thief must steal the plans or reproduce the plans and steal that separate object.

¹⁸⁴ Lederman, *supra* note 121, at 947.

¹⁸⁵ See *supra* note 103. Also, the state criminal statute of Delaware prohibits all four modes of acquisition and transmission. See *supra* notes 158-162 and accompanying text.

¹⁸⁶ Most of the state criminal law statutes were drafted in the late 1960's and early 1970's. Lederman, *supra* note 121, at 960. See *infra* note 187 and accompanying text.

¹⁸⁷ Today's economy renders most state statutes outdated for two reasons. The importance of information to the political, social, and economic environment has grown substantially in the past 20 years. Lederman, *supra* note 121, at 922. Information in all forms is a factor vital to the appropriate and efficient functioning of governmental, economic, and social systems. *Id.* Whereas the early 1900's were termed the "industrial revolution," the late 1990's has been termed the "information revolution." *Id.* at 923-25. This information revolution has had an enormous impact on the global business environment. *Id.* at 922-23. Information is not only the subject of transactions, but is also the driving force behind a variety of large industries. *Id.* at 925. Like natural resources and energy sources, information is an extremely important measurement of wealth and economic power. *Id.* at 926. Studies confirm that over 50% of the Gross National Product of the United States is directly or indirectly connected to the formation and distribution of information. *Id.* at 925. Coinciding with the information revolution, the strong competition in today's world

A third weakness is the lack of uniformity among the state statutes.¹⁸⁸ Some states adequately protect the information content, providing a comprehensive scope, coverage, and definition of qualifying proprietary information.¹⁸⁹ These same states, however, fail to proscribe the most common mode and form of misappropriation and theft.¹⁹⁰ The problem also reverses itself as many states provide a comprehensive definition of the proscribed modes of transfer but fail to cover the necessary proprietary information.¹⁹¹ Because of this deficiency, only three states provide a comprehensive and uniform approach.¹⁹²

The penalty provisions in the majority of state criminal law statutes present a fourth problem.¹⁹³ The majority of states penalize the theft and misappropriation of trade secrets and confidential business information with misdemeanor or low-class felony sanctions.¹⁹⁴ The combination of

markets has focused attention on securing the economic value of confidential commercial information. *Id.* at 926. Businesses have reacted by actively protecting the secrecy of important information such as business structures, development plans and business connections. *Id.* However, state law has failed to address the "information revolution" in criminal statutory legislation. The past 20 years have seen enormous technological advances in the acquisition and transmission of information. *Id.* at 923. Computer technology has provided the capacity for inexpensive data storage and processing. *Id.* at 922. Communication technology has allowed large amounts of data to be accessible and capable of transmission to immediate and remote locations. *Id.* See *supra* note 19 detailing the sophisticated methods of acquisition and transmission of confidential information.

¹⁸⁸ This is exactly the opposite of state civil law approaches, in which all states generally track the language of the UTSA producing uniform definitions and language throughout all of the states. See *supra* notes 22-23 and accompanying text.

¹⁸⁹ See *supra* notes 138, 143, 154 and 157.

¹⁹⁰ Florida and Minnesota are a representative example of the problems this causes. The language of the statute defining trade secrets covers business and economic information. Unless the theft occurs by corporeal acquisition or corporeal transmission, no criminal liability exists. See *supra* notes 142-143.

¹⁹¹ For example Texas and California prohibit corporeal acquisition, corporeal transmission, incorporeal transmission (exhibition or communication), and incorporeal retention. See *supra* notes 148-150. However, both Texas and California limit protection to only scientific or technical information. See *supra* note 152.

¹⁹² Colorado, Massachusetts, and Delaware proscribe all potential forms and modes of transfer while protecting all forms of commercial information. Businesses in these three states are well protected against theft and misappropriation of trade secrets and confidential business information. However, consider the deterrent effect on criminal homicide if only 6% of the states had statutes directly proscribing murder. In the area of trade secret protection, an adequate deterrent requires all states to adopt specific, comprehensive, and uniform criminal statutory protection.

¹⁹³ See *infra* note 194.

¹⁹⁴ One interesting phenomenon is that Colorado, an exceptional example of a state criminal statute in this area, provides only misdemeanor sanctions. COLO. REV. STAT. § 18-4-408 (West 1990). Arkansas and California also only provide misdemeanor sanctions, providing

all four limitations in current state law approaches to this problem demonstrate why companies have been reluctant to pursue prosecution of these offenses in the past.¹⁹⁵ To adequately protect the lifeblood of the U.S. economy, state law needs to respond by providing a comprehensive, powerful deterrent to the theft and misappropriation of trade secrets and confidential business information.

IV. MODEL CRIMINAL PENAL STATUTE

This Section of the Note proposes a model criminal statute that directly addresses the theft and misappropriation of trade secrets and confidential proprietary business information. Providing one single uniform and comprehensive statutory approach gives those states with no criminal statutory protection an example upon which to pattern future legislation.¹⁹⁶ Furthermore, states with current criminal statutory protection have the ability to amend and update their statutes to rectify the lack of uniformity, remove the limitations on the proscribed modes of acquisition and transmission, and to increase the scope and coverage

sentencing penalties of up to one year in prison. ARK. CODE ANN. § 5-36-107 (Michie 1997); CAL. PENAL CODE § 499C (West Supp. 1999). Most states punish the theft and misappropriation of trade secrets through felony sanctions. A number of states provide a minimum punishment of one year imprisonment and a maximum punishment of five years imprisonment. See CONN. GEN. STAT. ANN. § 53a-124 (West 1994); FLA. STAT. ANN. § 812.081 (West Supp. 1999); GA. CODE ANN. § 16-8-13 (1996); MASS. GEN. ANN. LAWS ch. 266 § 30 (West Supp. 1998); N.Y. PENAL LAW § 165.07 (McKinney 1999); 18 PA. CONS. STAT. ANN. § 3930 (West supp. 1998); TENN. CODE ANN. § 39-14-138 (1997); TEX. PENAL CODE ANN. § 31.05 (West 1994); WIS. STAT. ANN. § 943.205 (West Supp. 1999). The only states with severe penalty sanctions are Illinois and Minnesota. Illinois provides a minimum of four years imprisonment with a maximum of 15 years. 720 ILL. COMP. STAT. ANN. 5/15-8 (West 1993). Minnesota extends the maximum penalty to 10 years imprisonment. MINN. STAT. ANN. § 609.52(1) (West Supp. 1999). By contrast the EEA provides imprisonment up to 10 years for domestic offenders and 15 years foreign offenders. See *supra* note 107. Stiff felony penalties have the potential to deter criminal activity in a much greater fashion than the slap on the wrist provided by misdemeanor sanctions. See *supra* notes 24-33 and accompanying text.

¹⁹⁵ Businesses in one-half of the states have no criminal remedies available. Many state statutes do not cover business information. See *supra* notes 163-75. Other states fail to sanction the most common modes of acquisition and transition. See *supra* notes 163-75. These limitations make the investigation and prosecution of trade secret theft an expensive, time consuming, and risky proposition. Under the current statutory framework in the majority of states, prosecutors and companies recognize they face an uphill battle to successful prosecution. Many companies will absorb the loss rather than invest more money to wage an unsuccessful prosecution.

¹⁹⁶ Currently, close to 50% of states lack any criminal statutory protection for the theft and misappropriation of trade secrets and confidential proprietary business information. See *supra* note 124.

of information protected by expanding the existing narrow definition of trade secrets in the statutes.¹⁹⁷

The model criminal statute consists of six chapters. Chapter One identifies the prohibited conduct, affected parties, and penalty provisions.¹⁹⁸ Chapter Two postulates affirmative defenses to prosecution for violation of the statute.¹⁹⁹ Chapter Three provides criminal forfeiture conditions.²⁰⁰ Chapter Four furnishes devices to protect the confidentiality of the information during the criminal proceedings and prosecution.²⁰¹ Chapter Five details the construction and relation of this statute with other criminal and civil remedies available to the victim.²⁰² Chapter Five also incorporates a statute of limitations.²⁰³ Chapter Six categorizes and defines the relevant and important terminology used in Chapters One through Five.²⁰⁴ Chapters

¹⁹⁷ See *supra* notes 163-195 discussing the weaknesses in current state statutory law.

¹⁹⁸ This chapter is primarily modeled after 18 U.S.C.A. § 1832 (1996) (EEA). Modifications are made to include terms and phrases from various state statutes including California, Colorado, Delaware, Georgia, and Texas. See CAL. PENAL CODE § 499C (West Supp. 1999); COLO. REV. STAT. § 18-4-408 (West 1990); DEL. CODE ANN. tit. 11, § 857 (1995); GA. CODE ANN. § 16-8-13 (1996); TEX. PENAL CODE ANN. § 31.05 (West 1994). The penalty provisions are modeled following the approach of 18 U.S.C.A. § 1832 (1996) (EEA) and the state of Minnesota. See MINN. STAT. ANN. § 609.52(1) (West Supp. 1999).

¹⁹⁹ This chapter is modeled after the Pennsylvania approach, which is the only state or federal statute which explicitly provides for affirmative defenses to the theft of trade secrets and proprietary business information. 18 PA. CONS. STAT. ANN. § 3930 (West Supp. 1998). This chapter also follows California, Pennsylvania, and Wisconsin, stating explicitly what actions will not be considered an affirmative defense to alleviate violation and prosecution under the statute. See CAL. PENAL CODE § 499C (West Supp. 1999); 18 PA. CONS. STAT. ANN. § 3930 (West Supp. 1998); WIS. STAT. ANN. § 943.205 (West Supp. 1998).

²⁰⁰ This chapter is modeled after 18 U.S.C.A. § 1834 (1996) (EEA).

²⁰¹ This chapter is modeled after 18 U.S.C.A. § 1835 (1996) (EEA) and the state of Georgia approach. GA. CODE ANN. § 16-8-13 (1999).

²⁰² This chapter is modeled after 18 U.S.C.A. § 1838 (1996) (EEA) and state law approaches in Delaware, Massachusetts, and Wisconsin. See DEL. CODE ANN. tit. 11, § 857 (1995); MASS. GEN. ANN. LAWS ch. 266 § 30 (West Supp. 1998); WIS. STAT. ANN. § 943.205 (West Supp. 1998).

²⁰³ The majority of state civil trade secret statutes provide a statute of limitations. However, no state criminal law trade secret statutes affords any statute of limitations. With no state criminal law to model a statute of limitations upon, the Note incorporates the approach of the UTSA, discussed in *supra* note 22. Uniform Trade Secrets Act §§ 1-11, 14 U.L.A. 443 (1985).

²⁰⁴ This chapter combines aspects of § 1839 of the EEA with dozens of state law provisions, explanations, definitions, and terminology, most notably incorporating aspects of Colorado, Connecticut, Florida, Georgia, Maryland, Minnesota, New York, Oklahoma, Pennsylvania, and Wisconsin. See COLO. REV. STAT. § 18-4-408 (West 1990); CONN. GEN. STAT. ANN. § 53a-124 (West 1994); FLA. STAT. ANN. § 812.081 (West Supp. 1999); GA. CODE ANN. § 16-8-13 (1996); MD. CODE ANN. CRIM. LAW § 340(h)(11) (1992); MINN. STAT. ANN. §

One and Six represent the heart of the uniform, comprehensive, exhaustive and explicit nature of the statute. Furthermore, each Chapter contains a commentary section designed to explain each Chapter in more detail.²⁰⁵

The statute endeavors to explicitly delineate prohibited conduct and affected parties providing companies and individuals with prior notice of unlawful conduct. More importantly, the model criminal statute also endeavors to provide a powerful deterrent to the theft and misappropriation of trade secrets and confidential business information. The model statute strives to achieve this goal with rigid penalty provisions coinciding with comprehensive and definitive language clearly designating the proscribed modes of theft and misappropriation, while expanding the scope and coverage of the information content protected under the statute. The statute furnishes companies and state prosecutors with a powerful proactive weapon to combat the theft of trade secrets and the misappropriation of confidential business information. However, to properly utilize this weapon, all fifty states should adopt or amend current statutes to follow this model criminal statute.

A. Chapter 1: Theft of Trade Secrets and Confidential Proprietary Business Information

- (a) Any person who, with the intent to deprive, withhold or convert from the owner thereof, the exclusive use or control of a trade secret knowingly:*
- (1) steals, or without authorization appropriates, takes, carries away, transfers, or conceals, or by fraud, artifice, or deception acquires or obtains knowledge or information of the trade secret; or*
 - (2) without authorization accesses, copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, reproduces, transmits, delivers, sends, mails, communicates, discloses, exhibits, memorizes or conveys the trade secret; or*

609.52(1) (West Supp. 1999); N.Y. PENAL LAW § 165.07 (McKinney 1999); OKLA. STAT. tit. 21, § 1732 (West Supp. 1999); 18 PA. CONS. STAT. ANN. § 3930 (West Supp. 1998); WIS. STAT. ANN. § 943.205 (West Supp. 1998).

²⁰⁵ The commentary sections are employed to represent the history and explanation behind the provisions and serve a similar purpose to legislative history sections of federal and state law. Rather than repeat the analysis and assertions presented earlier in the Note, the commentary section will provide a brief explanation and refer the reader to earlier portions of the Note.

- (3) *receives, buys, uses or possesses the trade secret, knowing the same to have been stolen or appropriated, obtained or converted without authorization; or*
- (4) *completely or partially represents, depicts, describes, reflects or records the trade secret;*
- (b) *any person who attempts to commit any offense described in paragraphs (1) through (4); or*
- (c) *conspires with one or more persons to commit any offense described in paragraphs (1) through (4) and one or more of such persons do any act to effect the object of the conspiracy; or*
- (d) *wrongfully solicits another to commit any offense described in paragraphs (1) through (4)*

Commits the offense of the theft of a trade secret, and shall be fined not more than \$500,000 and imprisoned not more than 15 years, or both. Any organization that commits any offense described in subsections (a) through (d) shall be fined not more than \$ 5,000,000.

Commentary

Chapter 1 sets forth the prohibited conduct that triggers violation of the statute. Generally, the language in paragraph (1) seeks to prohibit corporeal acquisition and transmission.²⁰⁶ For example, paragraph (1) punishes physically walking away with the tangible object containing the trade secret. Paragraph (2) also seeks to prohibit corporeal acquisition and transmission.²⁰⁷ For example, paragraph (2) punishes the transmission of the trade secret into a separate tangible object which embodies the trade secret. For instance, photocopying or reproducing the trade secret in a separate tangible article is prohibited. Paragraphs (2) and (4) prohibit incorporeal transmission of the trade secret. For example, transmission by communication, exhibition, or disclosure violates the statute. Paragraph (2) also punishes incorporeal retention of a trade secret through the prohibition against memorization of the trade secret.²⁰⁸ With these nontraditional methods, the original trade secret

²⁰⁶ This provision tracks the majority of state law approaches to date. See *supra* notes 177-78.

²⁰⁷ Prior federal and state criminal statutory law has also addressed these concerns. See *supra* notes 59 and 179 and accompanying text.

²⁰⁸ The statute seeks to proscribe any and all means of acquisition and transmission of trade secrets and confidential commercial information. In today's technologically based economy, the theft of trade secrets will most commonly occur through incorporeal memorization and disclosure. This approach rectifies the problems witnessed by state law approaches in the past which failed to proscribe the most common means of stealing information. See *supra* notes 180-184.

never leaves the dominion or control of the owner, but the unauthorized exhibition or disclosure effectively destroys the value of the trade secret.²⁰⁹ The intent is to ensure that the theft of intangible information is prohibited in the same way that theft of physical items is protected.²¹⁰ Generally, paragraph (3) fills in any holes in acquisition by punishing unauthorized receipt, use, or possession. Paragraph (3) establishes a punishment for using improper means used to acquire the trade secret. Furthermore, the language of fraud and deception in paragraph (1) is meant to punish illegal business conduct, but also seeks to provide a disincentive for participation in immoral business conduct.

The language in paragraph (2) also serves to give the trade secret owner the right to control activities such as duplication, reproduction, exhibition and destruction, while punishing those who act against the interests of the owner. Paragraph (2) also attempts to stifle violations of confidential relationships through a prohibition against disclosure and communication. Finally the language of paragraph (2) applies to physical vandals and computer hackers who alter or destroy trade secrets. Prohibiting and punishing these acts is as important as theft or misappropriation to the protection of trade secrets.

Chapter 1 also outlines the affected parties under the statute. Subsection (b) covers the thief, while subsections (c) and (d) cover other parties involved in the theft. The language is deliberately broad, subject to two inherent limitations. First the person must knowingly commit the prohibited conduct. Second, the person must display criminal intent. These limitations are designed to limit its applicability in doubtful cases, where the person acted without knowledge that the actions were wrong. The limitations are aimed at preventing prosecution for accidental acquisition. A person who takes proprietary information or trade secrets because of ignorance, mistake or accident should not be prosecuted under this statute. For a person to be prosecuted, the person must know or have a firm belief that he has no lawful right to obtain the information.

Finally, the statute does not apply to innocent innovators or to persons who seek to capitalize on their lawfully developed knowledge,

²⁰⁹ Currently, very few states recognize this aspect. See *supra* notes 146-47.

²¹⁰ This remedies a recurring problem throughout current state criminal trade secret laws. A significant portion of the states adequately treat the theft of tangible property, although very few recognize the importance of protecting intangible property in the same manner as the protection of tangible property. See *supra* note 184.

skill, or abilities. For example, employees who change employers or start their own companies should be able to apply their talents without fear of prosecution. Chapter 1 attaches criminal liability for persons involved in either the solicitation of a theft of trade secrets or a conspiracy to unlawfully obtain a trade secret. Solicitation and conspiracy to steal trade secrets present problems on the same or greater scale than individual theft, and the statute will punish those persons severely. Finally, Chapter 1 pronounces the criminal sanctions for violation of the statute.²¹¹

B. Chapter 2: Defenses

- (a) *Defense: It shall be a complete defense to any prosecution under Chapter 1 of this statute for the defendant to show that the information comprising the trade secret was rightfully known or available to him from a source other than the owner of the trade secret.*
- (b) *In a prosecution for a violation of Chapter 1 of this statute, it shall be no defense that the defendant returned or intended to return the information or trade secret involved or that the defendant destroyed all copies or reproductions made.*

Commentary

Chapter 2 sets forth one affirmative defense available to the defendant to quash criminal prosecution. The language is constructed to prohibits prosecution if the trade secret or information was published, disseminated, disclosed or has otherwise become a matter of general public knowledge through the actions of the trade secret owner.

C. Chapter 3: Criminal Forfeiture

- (a) *The court shall order, in addition to any other sentence imposed, that the defendant forfeit to the state:*
 - (1) *any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and*
 - (2) *any property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violation.*

²¹¹ These sanctions are meant to provide a powerful deterrent to alleviate the problem witnessed by most state statutes in the past, misdemeanor and low-grade felony sanctions. See *supra* notes 193-194.

Commentary

Chapter 3 is designed to sanction the individual thief or enterprise devising the criminal theft by requiring any proceeds or property obtained or used to commit the theft to be forfeited to the state. Naturally, the state should return any appropriate property to the victim, such as the actual trade secret or confidential information. However, the state should be entitled to retain the excess property and proceeds to offset the expense of prosecution and to allow for adequate resources for the prosecution of future cases. These forfeiture provisions supplement, rather than replace, the authorized monetary punishments set forth in Chapter 1.

D. Chapter 4: Orders to Preserve Confidentiality

- (a) In a prosecution for any violation of this statute, a court shall preserve the secrecy of the trade secret or confidential information by reasonable means, which may include:*
 - (1) granting protective orders in connection with the discovery proceedings*
 - (2) holding in camera hearings*
 - (3) sealing the records of the proceedings*
 - (4) ordering any person involved in the litigation not to disclose any aspect of the trade secret or confidential information without prior court approval*

Commentary

This chapter alleviates the concerns of the trade secret owner. A public discovery process and prosecution inevitably will expedite the disclosure of the trade secret or confidential information to large numbers of individuals and groups. Exposure of the confidential trade secret destroys its worth and value. As an incentive for businesses to seek prosecution, the court shall take necessary and appropriate measures to protect the secrecy and confidentiality of the information. Without such a provision, the trade secret owner may be reluctant to cooperate in prosecutions.

E. Chapter 5: Construction with Other Laws

- (a) This statute shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by the United States Federal, State, commonwealth, possession, or territory law for the theft or misappropriation of a trade secret.*

- (b) *An action for theft or misappropriation of a trade secret shall be brought within three years after the theft or misappropriation is discovered or by the exercise of reasonable diligence should have been discovered. For the purposes of this section, a continuing theft or misappropriation constitutes a single claim.*

Commentary

Chapter 5 allows companies and businesses that are the victims of theft of trade secrets the ability to pursue state civil law remedies and federal criminal law remedies. This chapter also provides a statute of limitations. The statute of limitations tolls upon discovery of the theft or misappropriation of the trade secret or when the company, acting with reasonable diligence should have discovered the theft.

F. Chapter 6: Definitions

As used in Chapters 1 through 5:

- (a) *The term trade secret means all forms and types, whether the whole or any portion or phase thereof, of financial, business, scientific, technical, economic, or engineering information, including but not limited to: patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, codes, customer listings, supplier listings, sales listings, or any other information relating to any business or profession, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing; if*
- (1) *the owner has taken reasonable measures to keep such information secret; and*
 - (2) *the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by other persons or by the public.*
- (b) *The term "person" means any individual, sole proprietorship, partnership, corporation, business trust, estate, trust, limited liability company, association, joint venture, government, governmental subdivision or agency, or any other legal or commercial entity or enterprise.*
- (c) *The term "owner" means the person or entity in whom or in which rightful legal title or equitable title to, or license in, the trade secret is reposed.*

- (d) The phrase "without authorization" means without permission of the owner.
- (e) The phrase "intent to deprive" means to withhold the trade secret permanently or for such a period of time or under circumstances as to appropriate any portion of its economic benefit or value, or with the intent to restore the trade secret to the owner only upon payment of a reward or other compensation, or to dispose of the trade secret so as to make it unlikely that the owner will recover it.
- (f) The term "appropriate" means to exercise any control over the trade secret.

Commentary

Chapter 6 includes the definitions for terms and phrases used throughout the statute and should govern if any dispute arises as to the meanings of the terms or phrases used throughout the statute. The term "trade secret" is broadly defined to cover all confidential business information, whether tangible or intangible that accords the owner any competitive advantage over competitors or other persons. For example, the term trade secret encompasses strategic business plans, financial or sales data, reports or plans, manufacturing or production processes or techniques, marketing strategies, data compilations on consumers and suppliers and computer programs or codes. The term "trade secret" should be interpreted in an expansive way, subject only to the limitations of value and secrecy.²¹²

The requirement that the owner take reasonable measures to protect the secrecy of the trade secret should be construed to mean that the (1) owner regards or specifically identifies the trade secret or information as confidential, (2) the information is not available to anyone other than the owner or selected persons having access for limited purposes with the consent of the owner, and (3) the owner has not published or otherwise made the information known as a matter of general public interest. If the an owner fails to safeguard the trade secret, then no one can be rightfully accused of stealing or misappropriating the information.

²¹² The language of the statute remedies the main problem with prior state law approaches. Prior state law in the majority of jurisdictions limited prosecution to theft of purely scientific information. Prior state law approaches failed to explicitly cover business, economic, and commercial information. See *supra* notes 164-65.

V. CONCLUSION

Criminal theft and misappropriation of trade secrets and confidential business information represents the greatest single problem facing U.S. corporations in the next century. Businesses not only face the threat from foreign corporations and governments, but also from domestic rivals and competitors. To combat this serious problem and provide the maximum deterrent power, businesses, and companies need strong, comprehensive and proactive criminal laws. The federal government has addressed the problem of foreign corporations and foreign governments targeting U.S. corporations through the passage of the EEA. All fifty states have the ability and power to remedy the domestic side of the problem by adopting a uniform, comprehensive, and proactive criminal statutory approach. The states have the capability and the authority; all they need is the aspiration, desire and a set of proper tools to duplicate. The model criminal statute proposed in this Note furnishes the states with the tools necessary to enact comprehensive, proactive, and ground breaking criminal legislation.

Christopher A. Ruhl

