Fall 2001

Business War: Economic Espionage in the United States and the European Union and the Need for Greater Trade Secret Protection

Robert C. Van Arnam

Follow this and additional works at: http://scholarship.law.unc.edu/ncilj

Recommended Citation


Available at: http://scholarship.law.unc.edu/ncilj/vol27/iss1/5

This Comments is brought to you for free and open access by Carolina Law Scholarship Repository. It has been accepted for inclusion in North Carolina Journal of International Law and Commercial Regulation by an authorized editor of Carolina Law Scholarship Repository. For more information, please contact law_repository@unc.edu.
Business War: Economic Espionage in the United States and the European Union and the Need for Greater Trade Secret Protection

Cover Page Footnote
International Law; Commercial Law; Law
Business War: Economic Espionage in the United States and the European Union and the Need for Greater Trade Secret Protection

I. Introduction

The arrest of senior FBI official Robert Hanssen in February of this year reminded America of the dangers of foreign spying against United States national security interests. Economic espionage, however, is a less visible but more widespread form of attack that is conducted by employees against their own employers, by competing private companies, and by governments seeking to protect or expand their national economies. Economic espionage especially threatens intellectual property (IP), which has become the most valuable asset of global business. In 1995, for example, an employee of high-technology giant Intel attempted to steal the blueprints for the Pentium processor developed through years of research, development, and great cost. Although this employee was arrested prior to transmitting the data to an Intel competitor, he could have provided the information necessary to create an identical competing product and put a billion-dollar U.S. I


Within this Comment, the terms economic espionage and industrial espionage are used interchangeably and will be used to mean any illegal theft or misappropriation of business information, or attacks on communications systems by a business competitor or government entity.


company out of business. More recently, Microsoft's network was invaded by industrial hackers using a computer virus that allowed them to steal pending Microsoft products, which were traced to an electronic mail (e-mail) address in Russia. These attacks against two sophisticated technology giants demonstrate that all businesses are vulnerable to economic espionage.

In the United States and internationally, there is a dramatic rise in the need for trade secret law, rather than patents, to protect IP assets. The increasing value of trade secrets in the global economy and the simultaneous proliferation of technology have increased the opportunities and methods for conducting economic espionage. This Comment contends that economic espionage by private companies and national governments is dramatically increasing and that offensive economic espionage by the United States and its allies is detrimental to greater IP protection, to enhanced international cooperation against criminal organizations, and to economic growth. Furthermore, increased economic espionage creates a greater need for IP protection through trade secret law. Accordingly, this Comment recommends, first, that in the United States, individual states should adopt uniform civil and criminal trade secret laws modeled after the U.S. Uniform Trade Secrets Act (UTSA) and the Economic Espionage Act (EEA).

---

6 Michelle Cole, Proliferation of High Tech Firms Fosters Espionage, IDAHO STATESMAN, Apr. 27, 1997, at 10B.

7 Worming Out the Truth, ECONOMIST, Nov. 4, 2000, at 89. Microsoft was also recently the victim of spying by Oracle Corp. Oracle hired a detective agency to sift through Microsoft's lobbying firm's trash to acquire evidence that Microsoft was lobbying to influence the government's anti-trust case against it. Joe Lauria, Oracle Caper Lifts Lid on America's Corporate Spies, SUNDAY TIMES (London), July 9, 2000, at Business 6.


10 See infra notes 20-40 and accompanying text.

11 See infra notes 156-251 and accompanying text.

12 See infra notes 74-94 and accompanying text.

13 See infra notes 102-155 and accompanying text.
Second, in Europe, the European Union (EU) should explicitly recognize and protect trade secrets. Third, the United States and the EU should negotiate agreements to more effectively protect these rights based on criminal protections in the EEA and the World Intellectual Property Organization’s Model Provisions on Unfair Competition. Part II of this Comment explores the dramatic rise in global economic espionage and the threat it poses to private companies and national governments. Part III of this Comment reviews the federal law of trade secrets in the United States with focus on the UTSA and the EEA. In Part IV, this Comment examines the extent of international cooperation to protect trade secrets. Part V explores the protection of trade secrets in the EU and the war of economic espionage between the United States and the EU. Finally, in Part VI, this Comment recommends a framework on which the United States and the EU can increase cooperation on trade secret law and decrease their offensive use of economic espionage.

II. The Extent of the Problem

International economic espionage has existed for centuries. Over 1,500 years ago a Chinese princess hid silkworms in her hat and provided them to a man in India, thus revealing the secret of silk making to a foreign government. China lost another valuable industrial secret, the process for making high-quality porcelain, when a visiting French Jesuit memorized the process and described it in letters sent back to France. Today, industrial espionage affects the entire U.S. economy. A study by the American Society for Industrial Security (ASIS) found that in 1999, Fortune 1000 companies sustained losses of more than $45

---

14 *See infra* notes 198–204 and accompanying text.
15 *See infra* notes 20–40 and accompanying text.
16 *See infra* notes 41–155 and accompanying text.
17 *See infra* notes 156–197 and accompanying text.
18 *See infra* notes 198–251 and accompanying text.
19 *See infra* notes 252–304 and accompanying text.
21 *Id.* at 4.
22 Annually, *Fortune Magazine* ranks the top 500 and 1,000 U.S. companies in
billion from thefts of trade secrets.\textsuperscript{23} The greatest number of reported incidents came from the industrial areas of "high technology" and "services," but the greatest financial loss was in "manufacturing," averaging almost $50 million per incident.\textsuperscript{24} The number of jobs lost to industrial spying has been estimated at six million.\textsuperscript{25} The proliferation of global communication and information systems, including the Internet, has significantly increased the risks to corporate trade secrets. The world's reliance on technology to transact business will mean that financial loss from theft, misappropriation, and lost business opportunities will increase in the foreseeable future.\textsuperscript{26}

Generally, any country that competes in the world market has a motivation to spy on its foreign competitors.\textsuperscript{27} Economic espionage, however, is most prevalent in the world's most economically competitive nations and regions, including the United States, Asia, and Western Europe.\textsuperscript{28} In 1998, the FBI reported that there were twenty-three nations targeting the United States for economic information, twelve of which were

\textsuperscript{23} \textit{ASIS Report, supra} note 4, at 3. The \textit{ASIS Report} is based on a survey in which U.S. companies were asked to define their business and estimate their losses from the theft of trade secrets. Information was analyzed from the ninety-seven companies responding to the survey. The estimated loss of $45 billion is an extrapolation from data provided by the responding companies to all Fortune 1000 companies. \textit{Id.} at 25. The Institute of Intellectual Property Law informally estimates the loss to U.S. industry at $100 billion annually, factoring market losses and unrestricted technology transfers. Caroline Palmer, \textit{How to Spot Your Office Spy}, OBSERVER (London), Oct. 17, 1999, at Business 16.

\textsuperscript{24} \textit{ASIS Report, supra} note 4, at 6. The survey asked respondents to categorize their business into four industrial categories including: "High Technology," "Financial/Insurance," "Manufacturing," and "Services." \textit{Id.} There were 530 incidents in high technology and 536 incidents in manufacturing. \textit{Id.}

\textsuperscript{25} \textit{Economic Espionage Act: J. Hearing before the S. Select Comm. on Intelligence and the Subcomm. on Terrorism, Tech., and Gov't Info. of the Comm. on the Judiciary, 104th Cong. 2 (1996) (statement of Sen. Specter) (noting an ABC News Report of six million jobs lost).}

\textsuperscript{26} \textit{ASIS Report, supra} note 4, at 3.


\textsuperscript{28} \textit{Id.}
specifically targeting IP assets. For example, the French intelligence agency recently disclosed that it had bugged hotel rooms and the first-class cabins of Air France jets and substituted spies for flight attendants to eavesdrop on visiting foreign executives. Similarly, a Japanese company bought a scrap metal plant that contained damaged parts from a rival U.S. company’s machines to learn the weaknesses of that company’s equipment; the Japanese company then used this information in advertising to steal the lead in the market. Overseas, offices of U.S. companies are especially vulnerable to attacks by host governments or foreign companies.

Economic espionage is used not only to steal information, but also to weaken the capabilities and reputation of a competing company. Hackers are employed to deface or disable web sites, attack networks, or disrupt programs by adding code, this also allows competing companies to identify security weaknesses that are then used to gain access to more sensitive data. Despite these attacks, information losses are not consistently reported to U.S. federal or state law enforcement agencies. This is primarily due to: (1) the perception that IP theft is a low priority compared to more violent crimes; (2) the fear of adverse publicity or a required disclosure of trade secrets to the defendant; and (3) the desire to pursue civil remedies. Many of these fears are well-founded because information-loss incidents are difficult to investigate.

29 Freeh Statement, supra note 9, at 20.


33 Id. For example, Safeway’s online shopping site was hacked to obtain customer lists, and shoppers were then sent messages encouraging them to shop at other stores. The message appeared to have been issued by Safeway itself. John O’Reilly, Online Propaganda the Corporate Way, Nov. 29, 2000, at http://www.vnunet.com/analysis/1114674.

34 Lynch, supra note 32. Economic espionage by cyber attack is a global problem. “In December [of 2000] alone, websites of car manufacturers BMW (France), Renault (South Africa), Chevrolet (India and Argentina), [and] Opel (India) [had] all been defaced . . . .” Id.

35 ASIS REPORT, supra note 4, at 17.

36 Id. at 19.
Without complete cooperation of the injured party, trained staff of both the business and the law enforcement agency, and a timely response, investigations are severely hindered.\(^\text{37}\)

Nevertheless, the U.S. government and U.S. companies are not just victims of economic espionage but are actively seeking proprietary economic information themselves. For example, Germany is a "crucial field of operations for foreign spies."\(^\text{38}\) Large German corporations, such as BMW, Siemens, and Dasa, have been victims of industrial espionage.\(^\text{39}\) Enercon, a leading German manufacturer of wind energy equipment, recently alleged that the U.S. National Security Agency (NSA) intercepted communications regarding its new, cheap method for harnessing wind power and passed the information to a U.S. competitor that designed and patented an identical product.\(^\text{40}\)

### III. U.S. Trade Secret Law

#### A. Background

Historically, IP rights in the United States were based in federal patent and copyright protection, with trade secret law providing protection for "lesser" inventions that were unpatentable.\(^\text{41}\) Today, however, businesses are increasingly relying on trade secret law to protect proprietary information and new technological creations that are outside the scope of

\(^{37}\) _Id_.


\(^{39}\) Staunton, *supra* note 38, at 54.

\(^{40}\) _Id_. German intelligence chiefs in the state of Baden-Wuerttemberg, a major German industrial center, reported that two-thirds of all foreign espionage in 1997 was economic espionage. _Id_.

\(^{41}\) See Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 493 (1974) (stating that trade secret law protects and encourages the development of products of "lesser or different invention than might be accorded protection under the patent laws, but which items still have an important part to play in the technological and scientific advancement of the Nation"). _But see* J.H. Reichman, *Legal Hybrids Between the Patent and Copyright Paradigms*, 94 *Colum. L. Rev.* 2432, 2438 (1994) (arguing that legal theorists have underestimated the significance of trade secrets in intellectual property law). Information, data, or products may also be protected under the law of patents. *Roger M. Milgrim, Milgrim on Trade Secrets* § 8.02 (2001). The law of patents and trade secrets overlaps, but offer different levels of protection. _Id_.
traditional copyright and patent law. The use of trade secrets may be preferable to patent law because of the shorter life spans of technology products, the cost and delay in filing and defending patents, and the inadequacy of patent protection against modern theft. Significantly, federal patent law has recently been amended to require the public disclosure of pending patent applications eighteen months after the date they were filed. The essence of trade secret law is that the trade secret owner, who has worked to create value in its use, is rewarded with a commercial advantage over those who have not fairly developed similar knowledge. An individual or corporation maintaining a trade secret benefits from its rivals’ inability to duplicate the secret information, product, or process. Two famous examples include the formula for Coca-Cola that has been maintained in a bank vault in Atlanta, Georgia for over 100 years, and the recipe for Kentucky Fried Chicken that is kept in a secret location under guard. Trade secret law also imposes liability for disclosing or using another’s trade secrets.

---

42 E.g., Reichman, supra note 41 (arguing modern forms of innovation are not adaptable to traditional patent and copyright law); Pamela Samuelson et al., A Manifesto Concerning the Legal Protection of Computer Programs, 94 COLUM. L. REV. 2308 (1994) (analyzing why patent and copyright laws are ineffective to protect computer software programs).

43 Lamb, supra note 8, at 36–38. Companies have turned away from patent protection because they fear that the information and plans for their products on file with patent offices will be reviewed and copied by domestic and foreign firms. Id. Additionally, the life cycle of modern technology is short, rendering the seventeen-year U.S. protection meaningless. Id. Finally, patents are costly to file and defend and do not offer protection until they are officially filed, leaving the owner unprotected while an application is pending. Id.

44 35 U.S.C. § 122 (2001). Although there are exceptions and additional protections in the new legislation, this new requirement will result in increased disclosure of information not yet patented. Id.


47 Id.

48 RESTATEMENT OF TORTS § 757 cmt. c (1939).
B. The Civil Law of Trade Secrets

The first obstacle in protecting trade secrets is defining what they are. Until recently, the civil law of trade secrets was based in common law and equity.\(^49\) Many U.S. courts rely on the traditional definition found in the Restatement (First) of Torts: "[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 who do not know or use it."\(^50\) The Restatement of Unfair Competition expanded the definition of trade secrets to include all "economically valuable information."\(^51\) To maintain a common law cause of action in trade secret law, a plaintiff must show three elements: (1) the existence of a trade secret; (2) the improper disclosure or use of the trade secret; and (3) injury to the trade secret owner.\(^52\) The Restatement (First) of Torts identified six factors to be considered to determine whether information qualifies as a trade secret.\(^53\) No single factor is determinative, and courts must weigh all factors in their consideration.\(^54\)

---


\(^{50}\) RESTATEMENT OF TORTS § 757 cmt. b (1939).


\(^{52}\) RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 (1995).

\(^{53}\) RESTATEMENT OF TORTS § 757 cmt. b (1939). The following was provided as guidance:

An exact definition of a trade secret is not possible. Some factors to be considered in determining whether given information is one's trade secret are: the extent to which the information is known outside of his business; the extent to which it is known by employees and others involved in his businesses; the extent of measures taken by him to guard the secrecy of this information; the value of the information to him and to his competitors; the amount of effort or money expended by him in developing the information; the ease or difficulty with which the information could be properly acquired or duplicated by others.

\(^{54}\) DEBORAH E. BOUCHOUX, INTELLECTUAL PROPERTY: THE LAW OF TRADEMARKS,
First, although trade secret owners must protect their confidential information, courts do not require extreme and unduly expensive procedures to protect trade secrets against flagrant industrial espionage.55 In *E. I. duPont deNemours & Co. v. Christopher,*56 the Fifth Circuit set the standard for later trade secret protection, requiring “reasonable precautions” rather than an “impenetrable fortress” against any industrial espionage.57 Although secrecy need not be absolute, the greater the number of people who know the confidential information, the less likely it is to be a trade secret.58 Companies may freely disclose confidential information to their employees who have a “need to know,” but wider dissemination outside the employment relationship may defeat a trade secret claim.59 Generally, advising employees of the existence of trade secrets, limiting their access to the information on a “need to know” basis, and requiring them to sign confidentiality agreements constitute reasonable efforts to maintain secrecy.60

In terms of trade secrets transmitted via e-mail, courts may require advanced measures such as encryption and authentication systems to find that a plaintiff reasonably protected his secrets.61 The posting of a trade secret on the Internet destroys its secrecy and “prevents [a plaintiff] from further enforcing its trade secret

---

55 *E. I. duPont deNemours & Co. v. Christopher,* 431 F.2d 1012 (5th Cir. 1970), cert. denied, 400 U.S. 1024 (1971) (holding that plaintiff was not required to enclose its unfinished factory to protect it from defendant’s spying through the use of aerial photography).

56 *Id.*

57 *Id.* at 1017.

58 BOUCHOUX, supra note 54, at 342.


60 Religious Tech. Ctr. v. Netcom On-Line Comm. Servs., Inc., 923 F. Supp. 1231, 1254 (9th Cir. 1995) (holding plaintiff employer had made “more than an adequate showing” of reasonable efforts, citing the company’s use of locks and safes, logging and identifying the trade secret materials, limiting access to the materials, and requiring confidentiality agreements for all employees with access to the materials).

61 See *id.* at 1253–56.
rights in those materials" even if the trade secret was originally obtained by wrongful means.\textsuperscript{62} One court has even found that, in the absence of a confidential relationship or fiduciary duty, a plaintiff may not enjoin the disclosure of trade secrets on the Internet by a defendant who did not participate in their misappropriation.\textsuperscript{63}

Second, only "valuable" information constitutes a trade secret.\textsuperscript{64} To be valuable, a trade secret must not only have value to its owner, but must also have commercial value to competitors or others who might benefit from its use.\textsuperscript{65} Trade secret protection is afforded to processes and compilations of data as well as to information and tangible items.\textsuperscript{66} Courts have found trade secret rights in a computer software object code,\textsuperscript{67} detailed bid information regarding equipment leases,\textsuperscript{68} a compilation of changing retail sales information,\textsuperscript{69} and the process for converting

\textsuperscript{62} Id. at 1256. The court held that the defendant posting the plaintiff's information on the Internet was liable for misappropriation, but other use of the information was not actionable because the confidential information had become "generally known" and was no longer secret. Id. The court noted the danger of the anonymous defendant using the Internet to permanently destroy valuable trade secrets without an available remedy to the plaintiff. Id. For a further discussion of Religious Tech. Ctr., see Eugene A. Burcher and Anna M. Hughes, Religious Technology Center v. Netcom On-Line Communications Services, Inc.: Internet Service Providers: The Knowledge Standard for Contributory Copyright Infringement and The Fair Use Defense, 3 RICH. J.L. & TECH 5 (1997). The Internet age poses great challenges to protecting proprietary information. See, e.g., Ari B. Good, Trade Secrets and the New Realities of the Internet Age, 2 MARQ. INTELL. PROP. L. REV. 51 (1998); Ryan Lambrecht, Trade Secrets and the Internet: What Remedies Exist for Disclosure in the Information Age?, 18 REV. LITIG. 317 (1999).

\textsuperscript{63} Ford Motor Co. v. Lane, 67 F. Supp. 2d 745, 753 (E.D. Mich. 1999) (holding defendant's improper receipt and disclosure of plaintiff's trade secrets was not grounds for a prior restraint, which in this case would abridge defendant's rights under the first amendment).

\textsuperscript{64} BOUCHOUX, supra note 54, at 343.

\textsuperscript{65} Diamond v. T. Rowe Price Assoc., 852 F. Supp. 372 (D. Md. 1994) (holding that evidence failed to show value in trade secret to anyone but owner, so no protection was available).

\textsuperscript{66} BOUCHOUX, supra note 54, at 341–42.


wood pulp into paper—even though the elements of that process were all generally known. The ease of duplication by legal means, such as by "reverse engineering," would also make the original product unworthy of trade secret protection. Additional proper methods of discovering or acquiring a trade secret include independent invention, licensing from a lawful owner, observation of the item in public use, or acquisition from published literature.

C. The Uniform Trade Secrets Act

The evolution of trade secrets under state laws resulted in inconsistent protection across the United States. To harmonize these state laws, Congress enacted the UTSA in 1979. The UTSA protects information that is not generally known or readily ascertainable but has independent economic value and is the subject of reasonable efforts to maintain its secrecy. Like the

Digital Transactions, Inc., 920 F.2d 171 (2d Cir. 1990) (holding arrangement of four non-secret, publicly available computer programs that produced a previously unknown or used software process was a valuable trade secret).


71 Flotec, Inc., v. S. Research, Inc., 16 F. Supp. 2d 992, 1000 (S.D. Ind. 1998). The court in Flotec stated that, "The process known as 'reverse engineering,' in which a skilled person studies a product and figures out how to produce it, is permissible and even encouraged under trade secret law." Id. at 1000 (citing Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974)) (stating trade secret law "does not offer protection against discovery by fair and honest means, such as by independent invention, accidental disclosure, or by so-called reverse engineering, that is by starting with the known product and working backward to divine the process which aided in its development or manufacture").

72 BOUCHOUX, supra note 54, at 343.

73 RESTATEMENT OF TORTS § 757 cmt. b (1939).


76 UTSA § 1(4); BOUCHOUX, supra note 54, at 343. The UTSA defines trade secrets as follows:

"Trade Secret" means information, including a formula, pattern, compilation,
Restatement, liability under the UTSA requires the existence of a trade secret and its misappropriation by "improper means." Misappropriation can occur by unlawfully acquiring a trade secret or by the improper use or disclosure of a lawfully acquired trade secret, which are considered two separate causes of action. Third parties are liable for acquiring a trade secret, regardless of whether they actually used or disclosed the information, if they knew or had reason to know the information was acquired through unlawful means. Misappropriation by use or disclosure is actionable if the data was acquired in the context of a confidential relationship, such as employment, or through other improper means.

program, device, method, technique, or process that: (i) derives independent economic value, actual or potential, from not being generally known, 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.

The UTSA definition is broader than that of the Restatement because it includes information such as programs, methods, and techniques and it does not require, as does the Restatement, that information be in "continuous use in the operation of the business." The UTSA definition is broader than that of the Restatement because it includes information such as programs, methods, and techniques and it does not require, as does the Restatement, that information be in "continuous use in the operation of the business." Compare id. with UTSA § 1(4). Accord Phillips v. Frey, 20 F.3d 623 (5th Cir. 1994) (holding method of manufacturing and marketing plaintiff's hunting stand was a valuable trade secret that defendant misappropriated).

77 UTSA § 1(1). While the UTSA does not provide an exhaustive list of "improper means," it sets forth examples including: "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means." Id.

78 UTSA § 1(2). The misappropriation of a trade secret occurs when a person or entity discloses or uses a trade secret owned by another without that party's consent, uses improper means to gain knowledge of the secret, knew or should have known the trade secret was acquired by improper means, or knew or should have known that the trade secret was acquired under circumstances giving rise to a duty to maintain its secrecy. Id. Contra Ford Motor Co., 67 F. Supp. 2d at 753 (imposing no liability under the Michigan Trade Secrets Act for defendant's improper disclosure on the Internet of trade secrets he knew to be illegally obtained).

79 UTSA § 1(2)(i). Even if a trade secret were inadvertently acquired by a third party, that party would be liable if, before materially altering its position, it had actual or constructive knowledge of the trade secret and that its acquisition was a mistake. UTSA § 1(2)(ii)(C).

80 UTSA § 1(2)(ii)(B)(II).

81 UTSA § 1(2)(ii)(A).
Since 1979, forty-two states and the District of Columbia have adopted the UTSA.\(^8\) Even in these jurisdictions, however, the UTSA was modified prior to enactment, perpetuating inconsistent enforcement of trade secret law.\(^3\) The lack of uniformity in civil state trade secret law has had serious consequences. First, the nature of trade secrets and the injuries from their misappropriation result in a choice of law problem.\(^4\) In trade secret cases, it is difficult to ascertain where the injury or the act of misappropriation took place; the plaintiff’s development and safeguarding of a trade secret often occur in a different jurisdiction from where the defendant allegedly improperly acquired, used, or disclosed the information.\(^5\) The inconsistent application of trade secret protection also requires a national company with offices in multiple jurisdictions to enact the most restrictive and expensive confidentiality program to maintain its trade secrets.\(^6\) The choice of law problem is exacerbated where the parties are foreign companies and foreign trade secret laws are implicated. In *BP Chemicals Ltd. v. Formosa Chemical & Fibre Corp.*,\(^7\) a Taiwanese exporter of rayon and fiber contracted with a New Jersey company to fabricate certain chemical process vessels and

---


\(^9\) Id. at 1649. For example, the North Carolina Trade Secrets Act differs substantially from the UTSA. Id. at 1650 n.100; N.C. GEN. STAT. § 66.152–58 (1999).

\(^4\) Choice of law rules of a jurisdiction may require that it apply the substantive law of another state to the claim. RICHARD D. FREER & WENDY COLLINS PERDUE, CIVIL PROCEDURE 262 (2d ed. 1997).

\(^5\) See Lao, supra note 82, at 1672. The author’s hypothetical is instructive. She states:

For example, where the plaintiff was headquartered in Minnesota and had an office in Ohio (where the trade secret was developed and located), and where the defendant improperly used plaintiff’s trade secret in New York, it is not clear whether plaintiff was injured in Minnesota, Ohio, or New York, or perhaps all three states.

*Id.* Similarly, the planning and act of misappropriation may invoke the jurisdiction of several different states. *Id.* For a full discussion of the issues of jurisdiction and choice of law with IP right, see John N. Adams, *Industrial Property in a Globalized Environment: Issues of Jurisdiction and Choice of Law*, in INTERNATIONAL INTELLECTUAL PROPERTY AND THE COMMON LAW WORLD 251 (Charles E. F. Rickett & Graeme W. Austin eds., 2000).

\(^6\) Lao, supra note 82, at 1673.

\(^7\) 229 F.3d 254 (3d Cir. 2000).
heat exchangers for use in the construction of an acetic plant.\textsuperscript{88} Subsequently, a British company filed suit claiming that the Taiwanese company misappropriated trade secrets relating to the process for making acetic acid by copying elements of a plant design.\textsuperscript{89} The Third Circuit ultimately held that a state’s interest in protecting its citizens’ IP did not outweigh the interests of a foreign sovereign in establishing IP standards within its own borders.\textsuperscript{90} The court reached its holding only after determining where the alleged injury occurred and which of the laws of the three jurisdictions should govern the dispute.\textsuperscript{91}

The inconsistent protection of trade secrets may also violate U.S. treaty commitments. States that have adopted substantially modified provisions of the UTSA or that continue to apply Restatement rules may not meet the minimum standards for trade secret protection in multilateral treaties to which the United States is a party.\textsuperscript{92} Further, the lack of federal civil protection for trade secrets may indicate to foreign nations that such protection is not a U.S. priority and may undermine U.S. efforts to promote stronger trade secret laws internationally.\textsuperscript{93} Therefore, adherence to a uniform federal law, such as the UTSA, is necessary to provide consistent trade secret protection domestically and to further our interests and honor our commitments to protect IP internationally.\textsuperscript{94}

\textit{D. The Criminal Law of Trade Secrets}

Prior to 1996, existing criminal statutes indirectly punished

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{88} \textit{Id.} at 257.
\item \textsuperscript{89} \textit{Id.}
\item \textsuperscript{90} \textit{Id.} at 268.
\item \textsuperscript{91} \textit{Id.} at 264–67.
\item \textsuperscript{92} See Lao, \textit{supra} note 82, at 1677. The trade secret provisions of the North American Free Trade Agreement (NAFTA) and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) were based on the UTSA and are generally consistent with its provisions. Like the UTSA, NAFTA and TRIPS contain no requirement for the continuous use of a trade secret in one’s business as required by the Restatement. \textit{Id.} On TRIPS and NAFTA, see \textit{infra} notes 169–175, 180–186, respectively, and accompanying text.
\item \textsuperscript{93} See Lao, \textit{supra} note 82, at 1679.
\item \textsuperscript{94} \textit{Id.}; Cate, \textit{supra} note 74, at 716.
\end{itemize}
\end{footnotesize}
trade secret theft. The National Stolen Property Act (NSPA)\textsuperscript{95} prohibits the theft of tangible property containing trade secrets including documents or computer disks that are transported across state lines.\textsuperscript{96} A violation of the NSPA is not proven by the mere existence of a stolen trade secret in a state or country other than its original location; rather the prosecution must prove the item was physically transported and that the defendant knew the items were stolen.\textsuperscript{97} The government’s inability to prove these statutory elements resulted in ineffective trade secret prosecution under the NSPA.\textsuperscript{98}

The mail and wire fraud statutes were also used to prosecute the misappropriation of proprietary information.\textsuperscript{99} Unlike the NSPA, these fraud statutes are applicable to the theft of intangible rights, and they do not require proof that the defendant benefited from his crime.\textsuperscript{100} These statutes, however, are only applicable to trade secret theft through the use of the mail or wire services.\textsuperscript{101} Thus far, federal statutes have been generally ineffective at deterring industrial espionage and trade secret theft.

\subsection*{E. \textit{The Economic Espionage Act}}

The EEA\textsuperscript{102} is the first federal criminal law to protect trade secrets. Noting that foreign governments had redirected their espionage infrastructures at U.S. industry, the EEA was primarily designed to halt foreign espionage.\textsuperscript{103} The EEA, however, applies

\begin{footnotesize}
\end{footnotesize}
equally to the domestic theft of trade secrets.\textsuperscript{104} The EEA was developed from existing civil trade secret law, and it is both more expansive and narrower in scope than the UTSA.\textsuperscript{105} The EEA generally defines "trade secret" as all forms of business information that an owner has taken "reasonable measures" to keep secret that are not "generally known" or "readily ascertainable" by the public.\textsuperscript{106} Similar to the UTSA, the extent of trade secret protection must be reasonable under the circumstances.\textsuperscript{107} The EEA, however, more broadly defines the terms constituting trade secrets by expressly protecting intangible information and by protecting information regardless of how it is stored.\textsuperscript{108} Another expansive feature of the EEA is § 1837, which extends criminal punishment to conduct overseas if the defendant charged is bound by U.S. federal law or if "an act in furtherance of the offense was committed in the United States."\textsuperscript{109} This provision extends the jurisdictional reach of the U.S. Government to all U.S. citizens and corporations overseas and allows the United States to pursue trade secret theft abroad, so long as some part of the criminal activity is connected to the United States.\textsuperscript{110}

\textsuperscript{104} 18 U.S.C. § 1832.

\textsuperscript{105} Compare UTSA § 1(4), with EEA, 18 U.S.C. §§ 1831–1839.

\textsuperscript{106} 18 U.S.C. § 1839(3)(A)-(B). The Act provides a non-exhaustive list of types of "trade secrets" to guide those applying the statute. "[T]he term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, . . . programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing." Id. § 1839(3).

\textsuperscript{107} Id. § 1839. See Pioneer Hi-Bred Int'l v. Holden Found. Seeds, 35 F.3d 1226, 1235 (8th Cir. 1994).

\textsuperscript{108} 18 U.S.C. § 1839(3); Schwab & Porter, supra note 49 at 2, 3–4.

\textsuperscript{109} 18 U.S.C. § 1837(1)-(2) (1996). The Act applies to conduct proscribed in § 1831 if the act occurs outside the United States and:

(1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or (2) [if] an act in furtherance of the offense was committed in the United States.

\textsuperscript{109} Id.

\textsuperscript{110} See id.
In some respects, however, the EEA is more limited than the UTSA. The EEA only criminalizes the theft of trade secrets in or related to products "produced for or placed in interstate or foreign commerce." Moreover, the EEA only punishes intentional or knowing violations. Section 1831, which prohibits foreign espionage, requires that the actor intend or know the offense will benefit a foreign government or agent. Similarly, § 1832 punishes only the actor who "with 'intent' to convert a trade secret," "intending or knowing that the offense will injure the owner," "knowingly" misappropriates the trade secret by various acts of theft.

In terms of punishment and sentencing, individuals convicted of economic espionage under § 1831 are subject to maximum penalties of fifteen years in prison and fines of $500,000. Any organization found guilty under § 1831 "shall be fined not more than $10,000,000." The EEA provides that individuals convicted of trade secret theft under § 1832 will be "fined under this title or imprisoned not more than 10 years, or both." For organizations, § 1832 sets a maximum penalty of $5,000,000. In § 1834, the EEA also provides for the criminal forfeiture of any property taken in violation of the Act, or of any goods or property used to

---

111 18 U.S.C. § 1832(a) (emphasis added). It has been argued that this requirement may not protect a great body of valuable industrial information such as customer lists and the sources of raw materials. Joel M. Androphy et al., Criminal Prosecutions of Trade Secret Theft: The Emergence of the Economic Espionage Act, 38 Hous. Law. 16, 17 (2000).


113 18 U.S.C. § 1832(a). The government must establish three elements to prove its case. First, it must show the defendant intended to convert a trade secret and establish that the proprietary information constitutes a trade secret. Second, the government must show the defendant intended or knew that his conduct would injure the trade secret owner. The Act does not require the government to prove the defendant acted with malice or evil intent. Third, the government must show the defendant to have actual knowledge or belief to a substantial certainty that the information he is misappropriating is a trade secret. Ignorance, mistake, or accident are insufficient to prove knowledge under this element. Id.; Androphy et al., supra note 111, at 17.


115 Id. § 1831(b).

116 Id. § 1832(a).

117 Id. § 1832(b).

118 Id. § 1834(a)(1).
commit a violation of the Act.\textsuperscript{119} Although the EEA provides stiff penalties for IP crimes, sentencing has resulted in large monetary fines but limited prison sentences.\textsuperscript{120} Furthermore, the government has only used the criminal forfeiture option provided in § 1834 in three cases.\textsuperscript{121}

To date, the government has brought only eighteen cases under the EEA against defendant individuals and corporations.\textsuperscript{122} The dearth of prosecutions to date may have resulted from intentional selectivity by the government seeking to prosecute only clear cases of theft\textsuperscript{123} or, more likely, from inherent government and private sector limits on the EEA’s effectiveness.\textsuperscript{124} Of note,

\begin{itemize}
  \item \textsuperscript{119} \textit{Id.} § 1834(a)(2).
  \item \textsuperscript{120} Computer Crime and Intellectual Property Section, Department of Justice, \textit{Economic Espionage Act Case Summaries} [hereinafter EEA Case Summaries], at http://www.usdoj.gov/criminal/cybercrime/eeapub.htm (updated Oct. 5, 2001). While most convicted criminal defendants have received limited prison terms or probation, one defendant was sentenced to prison for fifty-four months, and another defendant was sentenced to prison for seventy-seven months. \textit{Id.} The light sentences for defendants convicted under the EEA are likely due, in part, to the frequency of guilty pleas by defendants seeking reduced prison terms. \textit{See id. Cf.} Chris Carr et al., \textit{The Economic Espionage Act: Bear Trap or Mousetrap?}, 8 \textit{Tex. Intell. Prop. L.J.} 159, 198 (2000) (noting that in several trade secret cases the government linked charges under EEA with other federal statutes “upping the ante” for defendants wishing to go to trial and encouraging them to plead guilty to lesser charges).
  \item \textsuperscript{121} Carr et al., \textit{supra} note 120, at 198.
  \item \textsuperscript{122} \textit{Id.} at 196.
  \item \textsuperscript{123} Joseph N. Hosteny, \textit{The Economic Espionage Act: A Very Mixed Blessing}, \textit{Intell. Prop. Today}, Feb. 1998, at 129, LEXIS, News Library, Intellectual Property Today (stating “the EEA is going to be selectively applied, at least for some time to come”). In many cases, the government waits to bring cases where a defendant’s criminal intent and knowledge are clear so that there is a high probability of conviction. \textit{Id.}
  \item \textsuperscript{124} \textit{See} Kent B. Alexander & Kristen L. Wood, \textit{The Economic Espionage Act: Setting the Stage for a New Commercial Code of Conduct}, 15 \textit{Ga. St. U. L. Rev.} 907 (1999). Government impediments to greater effectiveness include: prosecutors who are ill-prepared to prove the victim’s reasonable protection of trade secrets given their experience only in proving the criminality of a defendant’s conduct; the extremely technical nature of trade secret cases, which are difficult for prosecutors to prepare and too complicated for juries to comprehend; and the lower priority of trade secret thefts, as a white-collar crime, compared to more violent crimes. \textit{Id.} at 930–31. Private sector impediments include: the unwillingness of businesses to report violations for fear of required disclosure of trade secrets at trial; the inability of a victim in a criminal case to direct the litigation; the fear of discovery of misconduct by the defendant corporation; and the fear of bad publicity that can negatively affect public relations and advertising of
although many of the cases involve foreign nationals and businesses, the government has yet to bring charges for foreign espionage under § 1831. In general, EEA cases have included FBI undercover operations with recorded conversations to prove the necessary mens rea of the crime, and they have involved contractors, consultants, and former employees as defendants. All EEA cases have involved the theft of valuable trade secrets, including designs for a coal-mining machine, a Deloitte & Touche software program, CISCO optical networking software, and the product design for the Gillette Company’s new shaving system.

In United States v. Pin Yen Yang, the government brought one of the first EEA cases against foreign defendants. In Yang, a Taiwanese businessman, his daughter, and his “Four Pillars” the company’s products. Id. at 933–34. But see Dennis J. Kelly & Paul R. Mastrocola, The Economic Espionage Act of 1996, 27 NEW. ENG. J. ON CRIM. & CIV. CONFINEMENT 181, 190–91 (2000) (noting that despite disadvantages to pursuing criminal, rather than civil, claims, U.S. companies, especially smaller victim companies or larger companies with cases against “judgment-proof” civil defendants, will prefer to use the powers and resources of the federal government).


company were convicted of stealing Avery-Dennison Corporation's self-adhesive products and marketing them in Asia; the loss of these products was estimated at $50–60 million.\(^{134}\)

In December 1999, two individual defendants and three corporate defendants pled guilty and were sentenced to prison terms and fines totaling approximately $19 million.\(^{135}\) The founder of the three defendant corporations admitted stealing designs of machinery systems for the production and transmission of crude oil, manufacturing identical products, and selling these products overseas, including to an Iranian businessman in Sweden.\(^{136}\) Although charged under § 1832, the harmful impact of trade secret crime in both \(Y\text{ang}\) and the December 1999 pleas was not limited to the loss of valuable information by the victim corporation. These actions may also have directly supported foreign nations competing with U.S. industry.\(^{137}\)

In \textit{United States v. Hsu},\(^{138}\) one of the few reported cases under the EEA, the defendant, a technical director for a Taiwanese corporation, and Chester S. Ho, a biochemist and professor at National Chiao Tung University in Taiwan, were arrested for conspiring to steal trade secrets after a two-year FBI investigation.\(^{139}\) Hsu solicited executives of Bristol-Myers Squib Corporation who were posing as corrupt scientists trying to steal the formula for Taxol, a highly valuable anti-cancer drug.\(^{140}\)

\(^{133}\) \textit{Yang}, 74 F. Supp. 2d at 726.

\(^{134}\) \textit{Id.} (noting that the defendants in \textit{Yang} were continually supplied with proprietary information by an Avery-Dennison employee who acted as a "consultant" for Four Pillars for eight years).


\(^{136}\) \textit{Id.}

\(^{137}\) In 1999, an employee was arrested for stealing 3Com computer software codes while waiting to board a flight to Seoul, South Korea. Carr et al., \textit{supra} note 120, at 194–95 (citing \textit{United States v. Eun Joong Kim}, Criminal Case No. 99-CR-481 (N.D. Ill., filed July 1, 1999)). The theft and disclosure of this valuable information would have been devastating and, like any loss by a large company, would have negatively affected the U.S. economy. \textit{See id.} at 161–62.

\(^{138}\) 155 F.3d 189 (3d Cir. 1998).

\(^{139}\) \textit{Id.} at 191–93.

\(^{140}\) \textit{Id.} at 192.
Although the defendants were foreign nationals, they were charged under § 1832, the domestic provision of the law.\textsuperscript{141} Charges against Ho were eventually dismissed, but Hsu pled guilty and was sentenced to time served (two years) and a $10,000 fine.\textsuperscript{142}

The \textit{Hsu} decision is important because it established standards for future EEA cases. Protection of a plaintiff's trade secret during a prosecution under EEA has been a major concern for trade secret owners.\textsuperscript{143} Section 1835 allows courts to use their discretion to protect proprietary information.\textsuperscript{144} In \textit{Hsu}, the Third Circuit sought to balance the competing interests of a defendant's right to discovery and the victim's right to maintain the confidentiality of trade secrets.\textsuperscript{145} The Third Circuit reversed the district court's ruling allowing discovery of the trade secrets and remanded the case for an \textit{in camera} examination by the trial court to determine whether Taxol was, indeed, a trade secret.\textsuperscript{146} The Third Circuit held that the charges of conspiracy and attempt to steal trade secrets did not require a defendant's actual possession of the trade secret to prepare a defense.\textsuperscript{147} This ruling helped to allay long-held concerns that a victim of trade secret theft would be required to disclose the confidential information he sought to protect, thus defeating the main purpose of the EEA.\textsuperscript{148} Nevertheless, the continuing fear of disclosure of confidential information at trial may inhibit companies from reporting theft to U.S. law enforcement.\textsuperscript{149}

\textsuperscript{141} \textit{See id.} at 197.

\textsuperscript{142} \textit{Espionage Charges are Dropped Against Biochemist}, \textit{WALL ST. J.}, Feb. 2, 1999, at B5.

\textsuperscript{143} \textit{E.g.}, \textit{Susan V. Metcalfe, Protecting Trade Secrets: Is the Remedy Worse than the Wrong?}, 104 \textit{DICK. L. REV.} 503 (2000).

\textsuperscript{144} 18 U.S.C. § 1835 (Supp. V 1999) ("in any prosecution or other proceeding under this chapter, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets").

\textsuperscript{145} \textit{Hsu}, 155 \textit{F.3d} at 204–06.

\textsuperscript{146} \textit{Id.} at 205–06.

\textsuperscript{147} \textit{Id.} at 204.


\textsuperscript{149} \textit{Id.} For a discussion of how trade secrets are generally protected in the discovery
Courts applying the EEA have also had difficulty interpreting the vague language of the Act. In Hsu, on remand, the District Court for the Eastern District of Pennsylvania struggled with the concept of information that was "generally known" and "readily ascertainable" and therefore employed its own bio-technical experts to determine what information constituted trade secrets. The four experts disagreed as to what information should be protected and what information was generally known to the public. The defendants in Hsu also unsuccessfully raised the defense that the statute was "void for vagueness" based on these terms. Although there was sufficient evidence to prove the Hsu defendants were knowingly attempting to steal a trade secret, in subsequent cases, where a defendant's knowledge is less certain, prosecutors will likely face similar challenges concerning the vagueness of the act.

Therefore, trade secret protection in the United States is well established and has been enhanced by enactment of the UTSA and the EEA. Nevertheless, the inconsistency in state criminal law was, and is, an impediment to further protection of trade secrets and to greater international cooperation in this area. Although phase of civil and criminal cases, see Metcalfe, supra note 143.


151 Id. at 629. The four scientists disagreed as to the number of pages to be redacted to protect trade secrets, with two scientists finding that more than one hundred of the pages redacted by the other two scientists contained public information that should not have been redacted. Id.

152 Id. at 626.

153 Robin D. Ryan, The Criminalization of Trade Secret Theft Under the Economic Espionage Act of 1996: An Evaluation of United States v. Hsu, 40 F. Supp. 2d 623 (E.D. Pa. 1999), 25 DAYTON L. REV. 243 (2000). The author notes that in cases involving a completed theft, in which a defendant's knowledge that he is committing a crime is insufficient to establish guilt, courts may be required to evaluate the vague terms of the EEA. Id. at 260. "The void for vagueness doctrine requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement." Kolender v. Lawson, 461 U.S. 352, 357 (1983).

154 As of Spring 1999, "only thirty states [had] criminal laws addressing the theft and misappropriation of trade secrets." Christopher A. Ruhl, Corporate and Economic Espionage: A Model Penal Approach for Legal Deterrence to Theft of Corporate Trade Secrets and Proprietary Business Information, 33 VAL. U. L. REV. 763, 788–89 (1999) (proposing a model criminal penal code, based on the EEA, in order to protect trade secrets). Like state enactment of civil trade secret law, the state criminal statutes vary...
lack of uniform application and use impedes the effectiveness of both laws, they are models for greater trade secret cooperation internationally.\textsuperscript{155}

**IV. International Cooperation to Protect Trade Secrets**

The global development of IP is increasing dramatically. Information and communication technology is projected to surpass $3$ trillion by 2004.\textsuperscript{156} Nevertheless, IP protections, especially with regard to trade secret law, are not well established. Unlike patents and copyrights, trade secrets are not uniformly protected around the world.\textsuperscript{157} While trade secret protection is well established in many common law countries, such as the United Kingdom and parts of the British Commonwealth, such as Australia, trade secrets are not recognized in many countries due to cultural attitudes regarding ownership and use of valuable business information.\textsuperscript{158} The nature and extent of protection is also inconsistently applied in countries that have statutory or common
law trade secret remedies. For example, some countries do not protect non-industrial trade secrets such as computer programs or software, while others provide less protection for commercial information, such as consumer lists.

A. Multilateral Protection

Despite inconsistent national laws, the emerging multilateral regime to safeguard IP includes efforts to protect trade secrets.

1. The Paris Convention

The Paris Convention was the first international agreement protecting IP and focused on industrial property. The Paris Convention requires signatory nations to extend to foreign nationals the same IP protections that are provided to their own citizens. Although the Paris Convention continues to ensure that nations consistently enforce IP rights within their own borders, it permits and perpetuates weak national laws. Furthermore, the Paris Convention does not specifically address economic espionage. Article 10 on unfair competition only prohibits "[a]ny act of competition contrary to honest practices in industrial or commercial matters." The Paris Convention was designed to be flexible and allow signatory countries to have discretion in implementing national legislation; however, this has been ineffective in deterring economic espionage.

---

159 Id. at 411.
160 Id.
161 Id.
162 BOUCHOUX, supra note 54, at 439.
2. The Trade Related Aspects of Intellectual Property Agreement

The most extensive multilateral protection of IP was established by the Trade Related Aspects of Intellectual Property Agreement (TRIPS Agreement).\(^{169}\) The TRIPS Agreement was adopted in the Uruguay Round of Multilateral Trade Negotiations\(^ {170}\) in 1993. It requires member countries to protect against acquisition, disclosure, or use of an individual party’s undisclosed information.\(^ {171}\) Although the language in the TRIPS Agreement refers to “confidential information,” its definition is consistent with that of trade secrets. Specifically, the TRIPS Agreement protects information having commercial value, not in the “public domain,” whose owner has taken “reasonable steps” to maintain its secrecy.\(^ {172}\) The TRIPS Agreement also protects trade secrets, not as individual IP, but as a prohibition against unfair competition.\(^ {173}\) The TRIPS Agreement also enhances IP rights through enforcement mechanisms and remedies including a required recognition of third-party liability.\(^ {174}\) Nevertheless, the TRIPS agreement provides a broad exception, permitting members to adopt contrary national laws if necessary to protect “sectors of

---


\(^{171}\) TRIPS Agreement, supra note 169, art. 39.

\(^{172}\) Id. art. 39(2).


\(^{174}\) Id.; German Cavalier, Enforcement of Intellectual Property Rights, in INTELLECTUAL PROPERTY & INTERNATIONAL TRADE: A GUIDE TO THE URUGUAY ROUND TRIPS AGREEMENT, supra note 173, at 65. The World Trade Organization (WTO) Agreement governs the settlement of disputes, and all trade agreements concluded as part of the Uruguay Round, including TRIPS, are annexed to it. Thomas Pletscher, Basic Principles: Acquisition and Maintenance of Rights: Transitional Arrangements, in INTELLECTUAL PROPERTY & INTERNATIONAL TRADE: A GUIDE TO THE URUGUAY ROUND TRIPS AGREEMENT 15, supra note 173, at 18. See generally MILGRIM, supra note 41, § 9.08 (providing information as to how the WTO decides disputes).
vital importance to their socio-economic and technological development . . . .”

This exception may allow countries to avoid specific prohibitions against economic espionage that are not specifically forbidden by the agreement.

3. The World Intellectual Property Organization

The World Intellectual Property Organization (WIPO) is a global organization established in 1967 to administer several international treaties regarding IP, including the Paris Convention. WIPO’s purpose is to foster cooperation among states regarding IP, to encourage creative inventions and designs, and to modernize the administration and protection of industrial property and IP. As of March 2001, 177 countries belonged to WIPO. The WIPO Convention defines IP broadly to include rights related to any inventions, industrial property and designs, protection against unfair competition, and “all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields.”

4. The North American Free Trade Agreement

Another significant multilateral treaty protecting trade secrets is the North American Free Trade Agreement (NAFTA) between

---

175 TRIPS Agreement, supra note 169, art. 8.1.


178 Member States are listed at http://www.WIPO.org/members/index.html.

179 WIPO Convention, supra note 177, art. 2.
the United States, Canada, and Mexico. NAFTA, which entered into effect on January 1, 1994, is significant because it is the first international agreement to expressly provide protection for trade secrets. Under Article 1711, trade secret protection of parties is perpetual, as long as the information remains secret and unknown to the general public. NAFTA also requires the U.S. government to maintain the secrecy of confidential data submitted for product approval. This important provision helps to close a source of information to foreign governments and industrial spies who previously could mine U.S. government reports and administrative records for product information. However, the agreement is not without its flaws. Under NAFTA, a misappropriation of proprietary information is only actionable if the acquiring party knew, or was grossly negligent in failing to know, its actions were illegal; this is a higher standard than the requirement under U.S. tort law that a plaintiff prove a defendant’s knowledge or constructive knowledge.

B. The Anti-Bribery Conventions

Bribery of employees or government officials is a common form of economic espionage. Thus, public corruption and

---


181 NAFTA, supra note 180, art. 1711; MILGRIM, supra note 41, § 9.07. To ensure that the United States would not use compliance with IP laws as an excuse to restrict Canadian imports, Canada insisted that NAFTA contain “a warning” that IP rights would not themselves become a barrier to trade. NAFTA, supra note 180, art. 1701; Donald E. deKeiffer, U.S. Trade Policy Regarding Intellectual Property Matters, in INTERNATIONAL TRADE AND INTELLECTUAL PROPERTY 106 (George W. Stewart et al. eds., 1994).

182 NAFTA, supra note 180, art. 1711. Article 1711 offers protection for information or matters based on their relative, rather than absolute, secrecy, if their combination is not generally known, even if individual parts are publicly available, and if the information has actual or potential value. Id.

183 Id.

184 See id.

185 NAFTA, supra note 180, art. 1721.

186 RESTATEMENT OF TORTS § 757 cmt. b (1939).

187 Palmer, supra note 23, at 16. Bribery is a primary form of trade secret theft where disaffected or low-paid staff members are vulnerable to bribes of up to a full year’s salary for trash or material containing trade secrets. Id.
bribery laws have a large impact in deterring trade secret theft. 188 Recently, multilateral efforts have sought to discourage this long-standing practice in the international community. The Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (OECD Convention) 189 became effective in February of 1999. This multinational treaty, which was formulated by the Organization for Economic Cooperation and Development (OECD) 190 obligates signatory countries to make bribery of foreign public officials a criminal act. 191 The U.S. Congress ratified and implemented the OECD Convention by adopting amendments to the 1977 Foreign Corrupt Practices Act. 192 Although there are inherent deficiencies within the OECD Convention and its

188 See id.


190 The OECD is a Paris-based multilateral organization founded in 1960 with an annual budget of approximately $200 million. It consists of thirty member countries that together produce two-thirds of the world’s goods and services and includes the home countries of almost all multinational enterprises. OECD, About OECD, at http://www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-about-0-nodirectorate-no-no-no-0,FF.html (last visited Oct. 14, 2001).

191 OECD Convention, supra note 189. E.g., Barbara Crutchfield George et al., The 1998 OECD Convention: An Impetus for Worldwide Changes in Attitudes Toward Corruption in Business Transactions, 37 Am. Bus. L.J. 485 (2000). Currently, thirty-four countries have signed the Convention and implemented national legislation. These countries include: Argentina (Feb. 8, 2001); Australia (Oct. 18 1999); Austria (May 20, 1999); Belgium (July 27, 1999); Brazil (Aug. 24, 2000); Bulgaria (Dec. 22, 1998); Canada (Dec. 17, 1998); Chile (Apr. 18, 2001); Czech Republic (Jan. 21, 2000); Denmark (Sept. 5, 2000); Finland (Dec. 10, 1998); France (July 31, 2000); Germany (Nov. 10, 1998); Greece (Feb. 5, 1999); Hungary (Dec. 4, 1998); Iceland (Aug. 17, 1998); Ireland (signed, but has not ratified); Italy (Dec. 15, 2000); Japan (Oct. 13, 1998); Korea (Jan. 4, 1999); Luxembourg (Mar. 21, 2001); Mexico (May 27, 1999); The Netherlands (Jan. 12, 2001); New Zealand (signed, but has not ratified); Norway (Dec. 18, 1998); Poland (Sept. 8, 2000); Portugal (Nov. 23, 2000); Slovak Republic (Sept. 24, 1999); Spain (Jan. 14, 2000); Sweden (June 8, 1999); Switzerland (May 31, 2000); Turkey (July 26, 2000); United Kingdom (Dec. 14, 1998); United States (Dec. 8, 1998). Signature dates available at http://www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-document-88-3-no-6-7534-88,FF.htm (last visited Oct. 14, 2001).

implementation in many countries, these international and national prohibitions against bribery discourage a favorite method of illegally acquiring trade secrets.

On November 4, 1998, the Council of Europe (COE) adopted the Criminal Law Convention on Corruption, which becomes effective upon ratification by fourteen participating nations. The Convention on Corruption seeks to criminalize various corrupt practices, including active and passive bribery in both the private and public sectors, and to increase international cooperation in the prosecution of such offenses. As of March 3, 2001, nine member states had ratified the treaty. While a step in the right direction, the Convention on Corruption allows for circumvention of its prohibitions through declarations or reservations.

V. Trade Secret Law in the EU and the War of Economic Espionage

A. Trade Secret Law in the European Union

1. Background

The EU is one of the largest trading partners of the United States, and the EU’s IP laws directly impact the U.S. market. The EU evolved from the Treaty Establishing the European Economic Community (Rome Treaty), which was enacted on

193 George et al., supra note 191, at 515–18.
195 Id.
197 Convention on Corruption, supra note 194, art. 36. Signatories are allowed to declare that bribery of foreign officials is prohibited only if the official “acts or refrains from acting in breach of his duties.” Id. Reservations are also permitted for the bribery of foreign public assemblies. Id. art. 37.
March 25, 1957 to enhance economic coordination among western European nations. The Rome Treaty generally referred to the protection of industrial and commercial property, but did not create a central authority to protect IP rights. Without a central authority, member states were left to regulate their own national IP laws subject to EU "guidance." Over time, however, the EU sought to directly protect IP rights through competition laws, ensuring the free movement of goods and the consistent protection of IP rights among member countries. Under Article 36 of the Rome Treaty, the IP rights granted by any member state continue

200 The European Union originated from the European Community (EC), the group of European nations bound by the Rome Treaty. The Rome Treaty was amended by the SINGLE EUROPEAN ACT of Feb. 17 and 28, 1986, 1987 O.J. (L 169) 1, reprinted in 25 I.L.M. 503, and the TREATY OF AMSTERDAM AMENDING THE TREATY ON EUROPEAN UNION, THE TREATIES ESTABLISHING THE EUROPEAN COMMUNITIES AND CERTAIN RELATED ACTS, Oct. 2, 1997, 1997 O.J. (C 340) 1, reprinted in 37 I.L.M. 56 [hereinafter TREATY OF AMSTERDAM]. This treaty was separately joined by the European Union as the TREATY ESTABLISHING THE EUROPEAN COMMUNITY, Feb. 7, 1992, 1992 O.J. (C 224) 1, reprinted in 37 I.L.M. 56, as amended by the TREATY OF AMSTERDAM. The Treaty of Amsterdam was ratified on May 1, 1999. See France Ratifies EU Amsterdam Treaty Amid Criticism, AGENCE FRANCE-PRESSE, Mar. 3, 1999, LEXIS, News Library, Agence France-Presse File. There are four main EU institutions. The Council of Europe consists of representatives of the twelve member nations. Every six months, the presidency of the Council rotates. The Commission, consisting of seventeen members appointed for a four-year term, initiates and maintains Community policy and brings actions of breach of treaties before the European Court of Justice (ECJ). The ECJ, made up of thirteen judges and six advocates general, hears disputes among member nations, is the final authority on implementation of treaties, and interprets Community law. The European Parliament is the legislative body of the EC, which is made up of representatives from member nations. The sources of EU law include: internal treaties, which provide broad guidelines and apply Community law; regulations, which have general application and are binding in their entirety on member states; and directives, which are the main instruments to promote harmonization in corporate, tax and social laws. The directives are binding on member nations, but the methods of compliance and incorporation in national laws are left to the member nations; ECJ decisions are binding on member nations or the relevant parties to the dispute. The EU is also bound by international conventions. Clare Germain, EEC, in GERMAIN'S TRANSNATIONAL LAW RESEARCH IV-91 (1999). See, e.g., DOMNIK LASOK & JOHN WILLIAM BRIDGE, LAW AND INSTITUTIONS OF THE EUROPEAN COMMUNITIES (4th ed. 1987).

201 ROME TREATY, supra note 199, art. 30.

202 Id. art. 94. The Rome Treaty gave the EC Council the authority to direct "approximation of such laws" that directly affected "the establishment or functioning of the common market." TREATY OF AMSTERDAM, supra note 200, art. 94.

under the EU and are afforded the full force of law.  

2. Know-how

Trade secrets are only indirectly recognized as an IP right in the EU, in part, due to disagreements as to what information deserves protection. Article 81(3) of the Rome Treaty is the provision under which the EU has established most IP regulations. However, most EU member nations recognize the commercial value of confidential information that is the general foundation for trade secret protection. Similarly, EU regulations and directives indirectly recognize and protect “know-how” defined as “a package of non-patented practical information, resulting from experience and testing, which is secret, substantial and identified.” The three necessary elements of know-how are further defined as follows:

“secret” means that the know-how is not generally known or easily accessible; “substantial” means that the know-how includes information which is indispensable for the manufacture of the contract products or the application of the contract processes; “identified” means that the know-how is described in a sufficiently comprehensive manner so as to make it possible to verify that it fulfills the criteria of secrecy and substantiality.

Know-how rights are derived from patent law, where the inventor is forced to disclose secrets to receive patent protection.

---

204 Rome Treaty, supra note 199, art. 30; Cohen & Gutterman, supra note 157, at 429–30.
206 The Treaty provisions have been renumbered. Article 81(3) was formerly 85(3). Except where cited in earlier treaties, this paper will refer to the relevant article under its new number.
207 Id.
209 Id. art. 2, at 10.
EU law has recognized that an owner may license his patent and know-how to others without violating competition laws. In 1989, the EU granted an exemption from competition rules for pure know-how licensing agreements. In 1996, this regulation was incorporated into the Technology Transfer Regulation that exempts the licensing of patent and know-how and “ancillary provisions” regarding other IP rights. Thus, indirectly, the recognition and use of trade secret rights as know-how has been established in IP licensing in the EU.

3. Other EU Legislation

Other EU legislation specifically refers to, and may indirectly recognize, trade secret rights.

a. Data Protection

The EU provides extensive IP protection in the area of databases. On March 11, 1996, the European Council and European Parliament adopted the Directive on the Legal Protection of Databases (Database Directive) that extends a sui generis right over the contents of databases. The Database Directive also recognizes an existing trade secret right, primarily

---

211 Id.

212 Id. at 25–27. The sui generis right is:

[A] right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database.

213 Commission Regulation No. 556/89 of November 1988 on the application of Article 85(3) of the Rome Treaty to Certain Categories of Know-how Licensing Agreements, 1989 O.J. (L 61) 1; KORAH, supra note 210, at 288 n.3.

214 Id. at 1(1).


216 Id. at 25–27. The EU required the incorporation of the Directive’s provisions into national laws of member states. Id.

217 Id.
in member nations, stating that the Directive’s provisions are without prejudice to other laws regarding IP, unfair competition, or trade secrets.\textsuperscript{218}

\textit{b. Privacy}

On October 24, 1998, EU Directive 95/46/EC on the Protection of Individuals regarding the Processing of Personal Data and the Free Movement of Such Data (Privacy Directive) became effective.\textsuperscript{219} The Privacy Directive mandates regulatory controls over the processing and maintenance of personal data.\textsuperscript{220} Under this Directive, member states must enact national regulations that protect the confidentiality of communications by means of public telecommunications, networks, or services.\textsuperscript{221} Specifically, national regulations must ban the interception, storage, or surveillance of communication without the consent of the users concerned.\textsuperscript{222} The directive allows, by exception, national regulations that safeguard national security, defense, and investigation or prosecution of criminal offenses.\textsuperscript{223}

The Privacy Directive, however, qualified the access right of individuals to personal information stating, “this right must not

\begin{itemize}
\item \textsuperscript{218} Id. art. 13. Article 13 states, “This Directive shall be without prejudice to provisions concerning in particular copyright, rights related to copyright . . . unfair competition, \textit{trade secrets}, security, confidentiality, data protection and privacy, access to public documents, and the law of contract.” Id. (emphasis added).
\item \textsuperscript{221} Telecommunications Data Protection Directive, \textit{supra} note 220, at 1, 5.
\item \textsuperscript{222} Id.
\item \textsuperscript{223} Id. art. 14.1.
\end{itemize}
adversely affect trade secrets or intellectual property . . . ."224 Therefore, through current legislation regarding privacy, the EU indirectly recognizes trade secrets as an independent right. The current EU-U.S. debate225 over data privacy may help focus interest in cooperative efforts to protect trade secrets and decrease economic espionage.226

c. Utility Models

Many European member states also afford protection for "utility models," technical inventions that do not satisfy the elements of patent protection.227 Similar to U.S. trade secrets, the utility model offers a cheaper and faster method of protection, but one that is less secure than patents.228 Nevertheless, a common agreement in the EU for recognition of this right is problematic.229 Although utility models are common in European industry, this IP system does not exist in all EU member states, and its application among countries that do employ the system is inconsistent.230 In 1995, the EU produced a Green Paper proposing options for action on utility models.231 Respondents to the proposals have advocated greater harmonization among member nations, but have questioned an EU-wide system.232

Finally, the EU has recently recognized that the development and manufacture of flavoring substances are "trade secrets" and has recommended ways to protect them.233 Therefore, the

224 Privacy Directive, supra note 219, art. 41.
225 See Gregory Shaffer, Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards, 25 YALE J. INT’L L. 1, 27 (2000) (arguing that the U.S. system of ad hoc privacy protection in the private sector, which relies on market forces to ensure privacy rights, is directly in conflict with the EU’s regulation of private sector data collection).
226 Id.
227 Waterschoot, supra note 203, at 2–12.
228 Id.
229 Id.
230 Id.
231 Id.
232 Id.
233 Commission Recommendation 98/282 of 21 April 1998 on Ways in Which Member States and the Signatory States to the Agreement on the European Economic Area Should Protect Intellectual Property in Connection with the Development and
foundation exists for greater harmonization of EU IP rights and for the creation of a directive explicitly recognizing and protecting trade secrets. Although political and economic differences are obstacles to greater IP and trade secret protection, the EU's inconsistent recognition of IP rights and weak protection of trade secrets may divide the common market and impede greater trade with the United States.234

B. The War of Economic Espionage Between the United States and the EU

Despite increasing multinational efforts to protect trade secrets, the United States and its European allies continue to wage economic war via economic espionage.235 After the Cold War, many U.S. allies re-focused their foreign intelligence services on U.S. corporations.236 Current American allies, including France, Israel, Germany, South Korea, Russia, and Japan have been implicated in this spying,237 committed through wiretapping overseas phone calls, stealing computers, planting moles in U.S. companies, and monitoring “open source” materials such as commercial databases and trade journals.238 The U.S. government, however, is not just a victim. The extent of recent U.S. espionage was shown when U.S. intelligence agents were forced to leave France after allegedly stealing economic and political secrets,239 eavesdropping on the Japanese delegation at the U.S.-Japan automobile trade talks in Geneva in 1995,240 and were discovered hacking into the EU Parliament and Commission e-mail to access


234 KORAH, supra note 210, at 278.
237 Id. at 1116; SCHWEIZER, supra note 235, at 256.
238 Tucker, supra note 236, at 1123–25.
239 Douglas Waller, Spying: Halt! Friend or Foe?, TIME, Mar. 6, 1995, at 50.
240 Jim Landers, Foreign Spies Target Corporate Secrets, DALLAS MORNING NEWS, Oct. 7, 1996, at 1D.
economic information during the GATT trade talks.\textsuperscript{241}

This covert war was made public when EU Parliament ministers accused the United States and the United Kingdom of using the “Echelon” Spy System located in England to intercept European proprietary information and provide it to U.S. companies.\textsuperscript{242} Subsequently, the EU established a committee that is currently reviewing the matter to determine whether the rights of European citizens are protected from intrusion by intelligence services, whether European industry is at risk from global espionage, and whether encryption is adequate to guarantee privacy.\textsuperscript{243} Formally, the United States denied the allegations of spying. Former CIA Director James Woolsey, however, admitted that the United States spied on foreign corporations, but only to monitor sanctions and dual-use technology\textsuperscript{244} and to protect U.S. companies from bribery and corruption.\textsuperscript{245} The hypocrisy of the EU’s allegations was revealed when news sources publicly identified thirty other nations with eavesdropping capabilities, including five European countries, that engage in economic espionage.\textsuperscript{246} Most ironically, the French government, which

\begin{itemize}
\item\textsuperscript{242} Neil Buckley & Robert Graham, Europe: MEP’s to Vote on Probe of US-UK ‘Spying’ Satellite, FIN. TIMES (London), July 5, 2000, at 8.
\item\textsuperscript{243} Ian Lynch, EU Makes Blueprint for Echelon Inquiry, at http://www.vnunet.com/News/1110830 (Sept. 9, 2000).
\item\textsuperscript{244} Intelligence Gathering and Democracies: The Issue of Economic and Industrial Espionage, FED. NEWS SERVICE, Mar. 7, 2000, LEXIS, News Library, Federal News Service File (publishing the briefing of Dr. James Woolsey, Former Director of the Central Intelligence Agency). “Dual-use” technology includes products with legal, legitimate uses such as chemicals or supercomputers that can also be used to make or enhance illegal weapons of mass destruction. \textit{Id.}
\item\textsuperscript{245} \textit{Id.} Director Woolsey stated: “[T]he United States does not engage in industrial espionage in the sense of collecting or even sorting intelligence that it collects overseas for the benefit of and to be given to American corporations. . . . [Ninety-five] percent of our [economic] intelligence collection is from open sources. Five percent is essentially secrets that we steal. We steal secrets with espionage, with communications, with reconnaissance satellites.” \textit{Id.} The two claims of American spying on European companies included two French companies accused of bribing foreign officials to win contracts: Thompson-CSF allegedly was bribing Brazilian officials, and Airbus allegedly was bribing Saudi officials. \textit{Id.}
\item\textsuperscript{246} Duncan Campbell & Paul Lashmar, Revealed: 30 More Nations with Spy Stations, INDEP. (London), July 9, 2000, at 11.
\end{itemize}
claimed to have been victimized by Echelon, had a similar global network of spy satellites that collected foreign economic data. 247

Nevertheless, there is increasing cooperation between the United States and Europe to fight cyber-crime. In September of 2000, the United States sponsored a meeting of the G8’s Senior Law Enforcement Experts on Transnational Crime (Lyon Group)248 to discuss international IP crime.249 The meeting focused on the involvement of organized criminal groups in counterfeiting and pirating merchandise, but the delegates also discussed the possibility of mutual legal assistance and extradition agreements in the area of IP crime.250 The Lyon Group endorsed various recommendations, including sharing strategic intelligence concerning organized criminal groups and sponsoring an annual meeting on trends in IP crime and member countries' enforcement activities.251

VI. Recommendations and Conclusion

A. The Case for Greater Trade Secret Protection

1. Offensive Economic Espionage

First, nations could enhance their IP and trade secret rights by forming an agreement to prohibit offensive economic espionage. Proponents of offensive economic espionage argue that the U.S. government has long had legal authority to conduct such acts, and that the United States must continue these efforts to respond to foreign economic espionage.252 These proponents further contend that the U.S. government is exempted from civil or criminal

247 Id.
249 Id.
250 Id.
251 Id.
liability for economic espionage, and should therefore more directly assist private companies by disclosing to them any foreign trade secrets it discovers.\footnote{253}{Id. at 475. The author proposes government immunity under the UTSA and the EEA for the theft of foreign trade secrets based on the state action exemption in antitrust law. \textit{Id.}} Although historically the U.S. intelligence agencies have informally apprised U.S. businesses of foreign threats,\footnote{254}{Michael T. Clark, \textit{Economic Espionage: The Role of the United States Intelligence Community}, 3 J. INT’L LEGAL STUD. 253 (1997).} this expanded official role in offensive economic espionage is problematic. U.S. economic espionage risks retaliation from victim countries, damaged credibility when encouraging international agreements, and diminished respect for U.S. IP. Furthermore, conducting economic espionage might violate existing U.S. treaty commitments.\footnote{255}{Id.} Practically, this new role would require initial determinations of what constituted an “American” company and what foreign economic data was a trade secret and would be valuable to U.S. businesses.\footnote{256}{Id.}

Furthermore, offensive economic espionage during peacetime violates international law as a form of invasion on the territorial integrity and sovereignty of foreign nations.\footnote{257}{Myres S. McDougal et al., \textit{The Intelligence Function and the World Public Order}, 46 TEMP. L.Q. 365, 394 (1973). See also Quincy Wright, \textit{Espionage and the Doctrine of Non-Intervention in Internal Affairs}, in \textit{ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW} 3 (Roland J. Stranger ed., 1962). The principle of territorial integrity is recognized in Article 2(4) of the United Nations Charter. U.N. CHARTER art. 2, para. 4. Other scholars, however, believe that the prevalence of peacetime espionage has rendered it legal through constant practice. McDougal et al., \textit{supra}, at 393.} To date, however, espionage is not prohibited by any international convention because all nations maintain an interest in spying.\footnote{258}{W. Hays Parks, \textit{The International Law of Intelligence Collection}, in \textit{NATIONAL SECURITY LAW} 433–34 (John Norton Moore et al. eds., 1990). The author describes the inherently self-interested nature of domestic espionage law, stating:}

\begin{quote}
Each nation endeavors to deny intelligence gathering within its territory through domestic laws . . . [that] are promulgated in such a way as to deny foreign intelligence collection efforts within a nation’s territory without inhibiting that nation’s efforts to collect intelligence about other nations. No serious proposal has ever been made within the international community to prohibit intelligence collection as a violation of international law because of the tacit acknowledgement by nations that it is important to all, and practiced by each.
\end{quote}
the increasing importance of IP may force nations to redefine their traditional notions of the value of offensive economic espionage and determine whether it is in their political and economic interests to negotiate such a convention.

2. Vulnerability to Criminal Organizations

The failure of countries to criminalize the theft of IP and the increasing use of economic espionage by state and non-state actors increases vulnerability to criminal organizations. Increasingly, criminal organizations are infringing on IP rights to facilitate criminal enterprises involving guns, drugs, pornography, and terrorism. Former Attorney General Janet Reno stated that the failure to protect IP created “a nutrient environment for official corruption... and an increase in crimes financed by intellectual property theft.” Industrial espionage, however, has become an essential part of international business. To gain a competitive edge, corporations employ every means at their disposal, including the use of “retired” personnel from intelligence services, to learn the secrets of their business rivals. Driven by profit, such corporations may intentionally or unwittingly employ individuals or organizations that are fronts for criminal organizations or

Id.


260 Id. ¶ 5.

261 Id. ¶ 3.

262 Neil King Jr. & Jess Bravin, Corporate-Spying Firms Thrive: CIA Veterans, Dumpster-Divers Work in ‘Competitive Intelligence’: ‘If the Trash is on the Curb, It’s Fair Game,’ WALL ST. J. (Europe), July 4, 2000, available at 2000 WL-WSJE 21065482. For example, Motorola’s intelligence team is lead by an ex-CIA operative. Id. There are even trade associations for these professionals with thousands of members. Id. One such trade association, the Society for Competitive Intelligence Professionals [hereinafter SCIP], states its mission as “helping professionals develop expertise in creating, collecting, and analyzing information; disseminating competitive intelligence; and engaging decision-makers in a productive dialogue that creates organizational competitive advantage.” SCIP, About SCIP, at http://www.scip.org/about/mission.asp (last visited Oct. 12, 2001). U.S. and foreign companies use “competitive intelligence,” a dignified term for spying, to acquire information about competitors’ products clandestinely. Id. Corporate intelligence often includes gaining information legally by overhearing conversations at trade shows and airports, combing through U.S. Patent Office filings and the Internet, digging through the trash of a rival business, and taking photographs of their buildings and factories. Id.
foreign intelligence services.\textsuperscript{263} The increase in government-sponsored economic espionage makes trade secrets of private companies more vulnerable and increases their cost of protection from all sources of theft.\textsuperscript{264}

3. Economic Instability

Furthermore, weak trade secret laws and offensive economic espionage inhibit economic growth. Economically, IP laws provide a level playing field that induces, rather than inhibits, competition and invention.\textsuperscript{265} Specifically, "[e]ntitlements are allocated to specific creators, to safeguard their information against expropriation, so that bargaining can facilitate an exchange and a market is created."\textsuperscript{266} Enhanced trade secret protection discourages the "free-rider"\textsuperscript{267} and encourages companies or countries to create rather than copy an invention, thereby creating a greater number and variety of products for public consumption.\textsuperscript{268} Conversely, offensive economic espionage inhibits invention and negates the market incentive to create.\textsuperscript{269}

Theft of trade secrets through corruption and bribery also has economic consequences. Corruption makes economies less competitive because it undermines investment and leads to capital outflows.\textsuperscript{270} Furthermore, the more resources the U.S. government and U.S. companies spend on measures to perpetuate or defend

\textsuperscript{263} Robert L. Tucker, \textit{Industrial Espionage as Unfair Competition}, 29 U. TOL. L. REV. 245, 248 (1998). The recruitment and placement of moles in U.S. corporations has been reported to be "relatively easy." \textit{Id.} Foreign intelligence agencies routinely send students to study or work in America and report on scientific developments and classified technology. \textit{Id.} There is a close connection between IP-related crime, including economic espionage, and other criminal acts such as gun smuggling, drugs, money laundering, and even terrorism. \textit{See} Reno, \textit{supra} note 259.

\textsuperscript{264} ASIS REPORT, \textit{supra} note 4, at 3.


\textsuperscript{266} \textit{Id.}

\textsuperscript{267} \textit{Id.} A "free-rider" is an individual, company, or country that copies or steals the invention of another to reduce the time and cost of producing the product independently. \textit{See} \textit{id.}

\textsuperscript{268} \textit{Id.} at 102.

\textsuperscript{269} \textit{See} \textit{id.}

\textsuperscript{270} Helmut Sohmen, \textit{Critical Importance of Controlling Corruption}, 33 INT'L LAW. 863, 870 (1999).
against foreign espionage, the less money is available for public projects or tax incentives that might enhance private research and development. \(^{271}\) Therefore, greater protection of trade secret rights through international and bilateral agreements, and decreased offensive economic espionage would protect citizens and private companies and foster economic growth throughout the world. \(^{272}\)

**B. The Nature of an Agreement Between the United States and the EU**

1. **A Direct U.S.-EU Agreement on Trade Secrets**

The foundation for a U.S.-EU agreement on trade secrets and economic espionage exists in the 1999 Agreement on Mutual Recognition Between the European Community and the United States of America (Recognition Treaty). \(^{273}\) The Recognition Treaty specifies the conditions under which the two parties will accept or recognize the "conformity assessment procedures" of the other party's authorities. \(^{274}\) In Article 17, the United States and the EU agree to maintain the confidentiality of information exchanged under the Recognition Treaty, and not to disclose or permit their governmental bodies to disclose confidential information, including trade secrets. \(^{275}\) The Article is a direct recognition of and provision for trade secret rights, but each party is only required to protect these rights to the extent it is required to under its own laws. \(^{276}\) Thus, U.S. trade secret rights may still receive less protection in the EU under this agreement. \(^{277}\) Furthermore, the

---

\(^{271}\) Cf. Clark, *supra* note 254, at 290 (discussing the possibility that increased economic espionage activity may lead to a new economic Cold War).

\(^{272}\) See id.


\(^{274}\) Id. art. 2.

\(^{275}\) Id. art. 17. Article 17 states that "[N]either Party shall disclose to the public, nor permit a conformity assessment body to disclose to the public, information exchanged under this Agreement that constitutes trade secrets, confidential commercial or financial information, or information that relates to an ongoing investigation." Id.

\(^{276}\) Id. art. 3.

\(^{277}\) Id.
Recognition Treaty only applies to confidential information in conformity assessments, rather than a general agreement to respect and protect the other party's trade secrets.\textsuperscript{278} However, the Recognition Treaty provides a framework for additional agreements that more explicitly recognize and protect all trade secrets and prohibit offensive economic espionage.\textsuperscript{279}

To achieve the greatest protection for trade secrets, the proposed agreement should be based on the most expansive provisions of the UTSA and the EEA. Trade secrets could be defined, as in Article 1(4) of the UTSA, as any information that is not generally known or readily ascertainable but that derives independent economic value and is the subject of reasonable efforts to maintain its secrecy.\textsuperscript{280} Similarly, the agreement could define misappropriation as inappropriate acquisition, use, or disclosure.\textsuperscript{281} The criminalization of trade secret theft could be based on the EEA, including § 1837 that extends jurisdiction extraterritorially.\textsuperscript{282}

2. Additional Components of the Proposed Agreement

As part of a proposed trade secret agreement or other agreements protecting IP, the United States and EU should update their extradition treaties to provide for the extradition of non-state individuals wanted for economic espionage.\textsuperscript{283} Unlike the United States, many countries with civil law traditions, such as France, either do not extradite citizens charged with crimes in other countries or severely limit the conditions under which they extradite citizens.\textsuperscript{284} To achieve true cooperation, these nations

\begin{itemize}
\item \textsuperscript{278} \textit{Id.} art. 4.
\item \textsuperscript{279} \textit{Id.} art. 2.
\item \textsuperscript{280} UTSA § 1(4).
\item \textsuperscript{281} BOUCHOUX, \textit{supra} note 54, at 439.
\item \textsuperscript{282} 18 U.S.C. § 1837(1)-(2) (1996).
\item \textsuperscript{284} Joshua S. Spector, \textit{Extraditing Mexican Nationals in the Fight Against International Narcotics Crimes}, 31 U. MICH. J.L. REFORM 1018 n.90 (noting that many governments, particularly European and other civil law nations, including France,
should agree to extradite their own citizens charged with trade secret theft and expand their lists of extraditable crimes to include white-collar offenses such as industrial spying. Furthermore, European nations should follow the OECD and COE conventions on bribery and pass national legislation banning all corruption. A major obstacle to any proposed agreement is the close connection of the public and private sectors in Europe. Many European intelligence services claim that their budgets are indirectly funded by successful offensive economic espionage, which benefits their country’s economy. Thus, it is doubtful these foreign intelligence agencies will take steps to diminish this source of revenue until forced by national legislation.

3. Trade Secret Protection Through Unfair Competition Law

Alternatively, if the United States and the EU cannot agree to recognize trade secrets as IP, or to explicitly prohibit industrial espionage, then an agreement could seek to prevent disclosure and use of this information as unfair competition. The commitment to do so already exists. The TRIPS Agreement protects trade secrets through unfair competition by affording the trade secret owner the right to prevent others from disclosing or acquiring the confidential information without consent.

Germany, and Switzerland, refuse to extradite their nationals. Although all member states of the Council of Europe are signatories to the European Convention on Extradition, the treaty allows countries to define who constitutes a “national” and refuse to extradite these individuals if it is contrary to their legal traditions. European Convention on Extradition, Dec. 13, 1957, Art. 3(2), Art. 6, 359 U.N.T.S. 273, 280. See also Klosek, supra note 283, at 631; Hallee, supra note 283, at 683–84.

285 Klosek, supra note 283, at 655–56.
286 George et al., supra note 191, at 492–98.
287 Clark, supra note 254, at 288–89.
288 Id.
289 Id.
290 E.g., ANTITRUST LAWS & TRADE REGULATIONS § 5.04 (Matthew Bender & Co. 2d ed. 2000). But see Susy Frankel, Unfair Competition Law: Over Protection Stifles the Very Creative Force it is Supposed to Nurture, in INTERNATIONAL INTELLECTUAL PROPERTY AND THE COMMON LAW WORLD 269 (Charles E.F. Rickett & Graeme W. Austin eds., 2000) (arguing that the establishment of a separate law of unfair competition in New Zealand would chill competition).
291 TRIPS Agreement, supra note 169, art. 39(2).
Further, the foundation for protection through unfair competition exists in both U.S. and EU law. In the United States, courts have applied tort law, holding that misappropriating a competitor's business information constitutes unfair competition. Further, unfair competition law extends protection beyond trade secrets to other valuable proprietary information that does not rise to the level of trade secrets, and that is misappropriated through industrial espionage. As stated in Section V, the EU has historically based its IP protection on regulating competition. Article 82 of the EC Treaty prohibits the abuses of a "dominant" position held within the EU or a substantial part of it. The mere holding of an IP right, or the exercise of this right by a dominant firm, is not in itself an abusive act. The EU courts, however, have found IP abuses by dominant companies when there was an abusive registration of trademarks to divide markets, unfair licensing terms, and abusive and frivolous infringement actions.

The model for this agreement could be based on the WIPO Model Provisions on Protection against Unfair Competition. Article 6 of these Model Provisions defines, and prohibits, unfair competition with respect to "Secret Information" and provides a framework for greater trade secret protection and decreasing

292 Tucker, supra note 263, at 250.
293 RESTATEMENT OF TORTS § 757 (1939). The tort of unfair competition is focused on the nature of the party's conduct, rather than on the nature of the property misappropriated. The Restatement provides that wrongful misappropriation is independently tortious, even when information is not a trade secret. Id. cmt. b. Comment b states: "The tort of unfair competition is focused on the nature of the party's conduct, rather than the nature of the property misappropriated." Id.
294 See supra notes 198-251 and accompanying text.
295 Waterschoot, supra note 203, at 37.
296 ROME TREATY, supra note 199, art. 82.
298 GARZANITI, supra note 297, at 180 (citing CHRISTOPHER BELLAMY ET AL., COMMON MARKET LAW OF COMPETITION (Sweet & Maxwell, 4th ed. 1993)).
offensive economic espionage.300

C. Conclusion

Modern technology has facilitated a dramatic rise in economic espionage committed by private companies, criminal organizations, and national governments.301 Information is a vital asset of the global economy and is vulnerable to economic espionage if not adequately protected by national laws and international agreements.302 In response to these trends, the United States has enhanced its civil and criminal trade secret protection in federal laws.303 The inconsistent adoption of the UTSA under state laws, the limited use of the EEA, and the indirect and unreliable trade secret protection internationally, however, puts the confidential information of U.S. businesses at risk. Given the nature of technology, trade secret protection is becoming a common form of IP right and must receive commensurately heightened and explicit recognition in bilateral and multilateral agreements.304 To protect IP and sustain economic growth and trade, the United States and the EU should agree to increase their trade secret protection and reduce offensive economic espionage.

ROBERT C. VAN ARNAM

300 Id. art 6.
302 Id.
304 Lamb, supra note 8, at 36–38.