THE JOHN MARSHALL
REVIEW OF INTELLECTUAL PROPERTY LAW

PROTECTION OF U.S. TRADE SECRET ASSETS: CRITICAL AMENDMENTS TO THE ECONOMIC ESPIONAGE ACT OF 1996

R. MARK HALLIGAN

ABSTRACT

In order to protect the economic interests of the United States, the Economic Espionage Act was enacted in 1996. Although intended to prevent and deter trade secret theft, the EEA is limited to criminal prosecutions. Critical amendments to the EEA are required to create a civil cause of action in the new information-based economy and the international marketplace. The following proposed amendments to the EEA provide a federal civil cause of action, allowing companies to protect trade secret assets and to ensure the continued growth and protection of trade secret assets in the international marketplace.

Cite as R. Mark Halligan, *Protection of U.S. Trade Secret Assets: Critical Amendments to the Economic Espionage Act of 1996*, 7 J. MARSHALL REV. INTELL. PROP. L. 656 (2008).

PROTECTION OF U.S. TRADE SECRET ASSETS: CRITICAL AMENDMENTS TO THE ECONOMIC ESPIONAGE ACT OF 1996

R. MARK HALLIGAN*

INTRODUCTION

On October 11, 1996, President Clinton signed The Economic Espionage Act of 1996 ("EEA") into law.[1] The EEA made theft of trade secrets a federal criminal offense.[2] Nearly twelve years after this ground-breaking legislation, trade secret theft and economic espionage continues to run rampant.[3] United States' industry has become the equivalent of a giant cookie jar permitting foreign agents and unscrupulous competitors to steal American know-how with a low probability of detection or prosecution.[4] The protection of trade secret assets is in the national economic interest of the United States.[5] The time has come for the enactment of a

---

* R Mark Halligan is a Partner in the Chicago office of Lovells LLP. Mr. Halligan is on the Adjunct Faculty at John Marshall Law School where he teaches advanced trade secrets law and trade secrets litigation. Mr. Halligan is the Chair of the ABA IPL Committee on Trade Secrets; Chair of the AIPLA Committee on Trade Secrets and he is a Past President of the Intellectual Property Law Association of Chicago ("IPLAC").

[1] Pub. L. No. 104-294, 110 Stat. 3488 (1996) (codified at 18 U.S.C. §§ 1831–39 (2006)).

[2] *Id.* at sec. 101, § 1832 (a), 110 Stat. at 3489 (codified at 18 U.S.C. § 1832).

[3] NAT'L INTELLECTUAL. PROP. LAW. ENFORCEMENT COORDINATION COUNCIL, REPORT TO THE PRESIDENT AND CONGRESS ON COORDINATION OF INTELLECTUAL PROPERTY ENFORCEMENT AND PROTECTION viii (2008), *available at* www.commerce.gov/NewsRoom/TopNews/ssLINK/prod01_005189 [hereinafter NIPLECC Report]. In the Letter of Transmittal, Chris Isreal, U.S. Coordinator for International Intellectual Property Enforcement, states: "[r]ampant piracy remains all too common in major markets throughout the world, and IP theft continues to be a serious problem here at home." *Id.*; *see also* Ariana Eunjung Cha, *Even Spies Embrace China's Free Market: U.S. Says Some Tech Thieves Are Entrepreneurs, Not Government Agents*, WASH. POST, Feb. 15, 2008, at D1 (quoting Assistant Attorney General Kenneth L. Wainstein as saying: "there are a number of countries that have proven themselves particularly determined and methodical in their espionage efforts").

[4] *See* Michael L. Rustad, *The Negligent Enablement of Trade Secret Misappropriation*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 455, 463 (2006) (noting that there are over 3,000 Chinese "front companies" that attempt to steal U.S. technologies).

[5] 142 CONG. REC. S12,207 (1996) (statement of Sen. Specter); *Id.* at H10,461 (statement of Rep. Hyde) ("In my opinion, our economic interests should be seen as an integral part of [the country's] national security interests, because America's standing in the world depends on its economic strength and productivity."); Press Release, U.S. Dep't of Commerce, Administration's Annual IP Report: IP Related Prosecutions Up, Focus on Health and Safety Redoubled (Feb. 11, 2008), *available at* http://www.commerce.gov/NewsRoom/PressReleases_FactSheets/PROD01_005190 [hereinafter Press Release on IP Report] (quoting Secretary of Commerce Carlos M. Gutierrez as stating: "[c]reativity and innovation are the lifeblood of the American economy, and intellectual property protection is vital to ensure our economic health now and for the future").

> In an increasingly complex and competitive economic world, intellectual property forms a critical component of our economy. As traditional industries shift to low-wage producers in developing countries, our economic edge depends to an ever-increasing degree on the ability of our businesses and inventors to stay one step ahead of those in other countries. And American business and inventors have been extremely successful and creative in developing intellectual property

federal trade secrets statute. This Article recommends amendments to the Economic Espionage Act of 1996 to create a civil cause of action. The proposed amendments to the EEA are set forth in Appendix A to this article.

I. THE LEGISLATIVE HISTORY OF THE EEA

The EEA legislative history illustrates that the Economic Espionage Act of 1996 was enacted to fill existing gaps in existing federal and state law and to create a national scheme to protect U.S. proprietary economic information.[6] Congress recognized that protecting U.S. trade secrets was necessary to "maintain our industrial and economic edge and thus safeguard our national security."[7] According to Senator Herbert H. Kohl, a company's proprietary information is incredibly important.[8]

> [B]usinesses spend huge amounts of money, time, and though developing proprietary economics information – their customer lists, pricing schedules, business agreements, manufacturing processes. This information is literally a business's lifeblood. And stealing it is the equivalent of shooting a company in the head. . . . The economic strength, competitiveness, and security of our country relies [sic] upon the ability of industry to compete without unfair interference from foreign governments and from their own domestic competitors. Without freedom from economic sabotage, our companies loose [sic] their hard-earned advantages and their competitive edge.[9]

These observations twelve years ago ring even more true today. U.S. corporations are now immersed in intense global competition and American industry is being challenged both at home and abroad.[10] Today, it is estimated that as much as 80% of the assets of new economy companies are intangible assets and the vast

---

> and trade secrets. America leads the nation's [sic] of the world in developing new products and new technologies. Millions of jobs depend on the continuation of the productive minds of Americans, both native born and immigrants who find the freedom here to try new ideas and add to our economic strength.

142 CONG. REC. S12,207.

[6] H.R. REP. NO. 104-788, at 4 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4022–23.

[7] S. REP. NO. 104-359, at 11 (1996); *see* 142 CONG. REC. H10,461 (1996) (statement of Rep. Hyde) ("In my opinion, our economic interests should be seen as an integral part of [the country's] national security interests, because America's standing in the world depends on its economic strength and productivity.").

[8] 142 CONG. REC. S740 (daily ed. Feb. 1, 1996) (statement of Sen. Kohl),

[9] *Id.*

[10] *See* THOMAS L. FRIEDMAN, THE WORLD IS FLAT: A BRIEF HISTORY OF THE TWENTY-FIRST CENTURY (2005) (describing the effects of globalization on American culture and business); Daniel Altman, *Managing Globalization: Has it Hurt U.S. Workers?*, INT'L HERALD TRIB., Apr. 17, 2007, http://www.iht.com/articles/2007/04/17/business/glob18.php ("Looking at the statistics, it is hard to argue that globalization has been a destructive force in the American labor market."); Michael A. Fletcher, *Globalization Requires Safety Net, U.N. Says*, WASH. POST., Jul. 2, 2008, at D3 ("[g]reater government intervention is needed to moderate the severe economic swings and inequalities that seem to be an unavoidable byproduct of globalization").

bulk of intangible assets are trade secret assets.[11] Each year the protection of trade secret assets is becoming more important to the competitiveness of U.S. industry and each year the protection of trade secrets is becoming more important to the economic strength and well being of the nation.[12]

These structural changes have been accompanied by a computer revolution and transition to the Information Age.[13] The power of computer technology has increased exponentially, resulting in more powerful means for the theft and transfer of proprietary information.[14] The rapid growth of the Internet is a reflection of this boom.[15] In fact, the corollary is also true: the Internet is now a tool for the destruction of trade secret assets.[16]

Computers facilitate the instant copying and transfer of proprietary information surreptitiously.[17] One can download trade secret information from the company's computer to a thumb drive or other media, transfer proprietary information to other computers, upload proprietary information to the Internet, and transmit the purloined information anywhere in the world within minutes. The receiving party can do the same thing -- and the cycle can be repeated -- over and over again. Within days or even hours, a U.S. company can lose complete control over its trade secret assets forever.[18]

---

[11] *See* MARGARET M. BLAIR & STEVEN M.H. WALLMAN, UNSEEN WEALTH: REPORT OF THE BROOKINGS TASK FORCE ON INTANGIBLES (2001) (assessing the importance of intangible assets in U.S. economic growth); Nir Kossovsky, *Accounting for Intangibles: From IP to CEO*, PAT. STRATEGY & MGMT. Dec. 2007, at 3, 3 ("[A]mong the S&P 500 companies, intangible assets represent anywhere from 60-80% of the market capitalization . . . ."); Margaret M. Blair, *New Ways Needed to Assess New Economy*, L.A. TIMES, Nov. 13, 2000, at 7.

> Depending on the measure used, at least 50%, and possibly as much as 85%, of the assets and other sources of value in the corporate sector do not appear on the books of corporations. In some firms, the gap between so-called "book" value (what the accountants say the assets of the firm are worth) and the firm's market value is modest, but in others the gap is as much as 95%.

Id.

[12] *See* NIPLECC Report, *supra* note 3, at 45 ("Protecting IP . . . is crucial to increasing trade and competing in the global economy.").

[13] Brian M. Hoffstadt, *The Voyeuristic Hacker*, J. INTERNET L., July 2007, at 1, 1 (noting that the computer ushered in the Information Age).

[14] *See* 2 JOHN J. FALVEY, JR. & AMY M. MCCALLEN, INTERNET LAW AND PRACTICE § 26:6 (2008) ("The widespread use of the Internet, coupled with specific technologies that have developed to facilitate copying, makes intellectual property theft easier than ever.").

[15] *Id.* ("Growth in use of the Internet has also offered inviting opportunities for intellectual property crimes.").

[16] *Id.* ("[T]he Internet has also been used as a vehicle to facilitate the theft of trade secrets.").

[17] *Id.*

[18] Albert P. Halluin & Lorelei P. Westin, *Nanotechnology: The Importance of Intellectual Property Rights in an Emerging Technology*, 86 J. PAT. & TRADEMARK OFF. SOC'Y 220, 225 (2004); Bruce T. Atkins, Note, *Trading Secrets in the Information Age: Can Trade Secret Law Survive the Internet?*, 1996 U. ILL. L. REV. 1151, 1154 (1996); R. Mark Halligan, *The Recently Enacted Economic Espionage Act, Which Makes Trade Secret Theft a Federal Crime, Specifically Addresses Theft Perpetrated via the Internet*, NAT'L L.J., Dec. 9, 1996, at B6; *see also* Elizabeth A. Rowe, *Introducing a Takedown for Trade Secrets on the Internet*, 2007 WIS. L. REV. 1041, 1042–43 (2007) (noting that trade secrets that turn up on the Internet are no longer secrets).

> Although trade secrets can be a powerful arsenal in the protection of intellectual property rights, it is becoming more and more difficult to keep such knowledge confidential. Because of the increased mobility of employees and the

Before the EEA, federal prosecutors relied primarily upon the National Stolen Property Act[19] and the wire and mail fraud statutes to commence criminal prosecutions for trade secret theft. Both statutes were ineffective.[20] On the day the EEA was enacted, President Clinton issued the following statement:[21]

> Trade secrets are an integral part of virtually every sector of our economy and are essential to maintaining the health and competitiveness of critical industries operating in the United States. Economic espionage and trade secret theft threaten our Nation's national security and economic well-being.
>
> Until today, Federal law has not accorded appropriate or adequate protection to trade secrets, making it difficult to prosecute thefts involving this type of information. Law enforcement officials relied instead on antiquated laws that have not kept pace with the technological advances of modern society. This Act establishes a comprehensive and systemic approach to trade secret theft and economic espionage, facilitating investigations and prosecutions.
>
> This bill also strengthens protection for our national information infrastructure by eliminating gaps in the criminal laws covering attacks against computers and the information they contain. Importantly, it does so without impeding the development of legitimate uses of the information infrastructure.
>
> This Act will protect the trade secrets of all businesses operating in the United States, foreign and domestic alike, from economic espionage and trade secret theft and deter and punish those who would intrude into,

---

> accessibility of the internet, the ease of getting information makes trade secrets difficult to defend. Few venture capital firms will risk placing investments on companies that rely primarily on trade secrets. Because of the easy accessibility to important information, many emerging technology companies rely on patents to protect their intangible asses.

Halluin & Westin, *supra*, at 225 (footnote omitted).

> Perhaps most daunting for trade secret owners, however, is that they are powerless to counter industrial espionage and underhanded tactics on the Internet to exploit trade secrets, as even the strictest security measures in the workplace will not stop an ill-intentioned employee from disclosing valuable trade secrets in cyberspace. After all, with a little know-how and the use of any of a number of computers in a multitude of locations, disclosing a secret in cyberspace takes a matter of seconds.

Atkins, *supra*, at 1154.

[19] *See* 19 U.S.C. §§ 2314–15 (2006).

[20] *See* Rustad, *supra* note 4, at 465–66.

[21] Press Release, White House Office of the Press Sec'y, Statement by the President (Oct. 11, 1996), *reprinted in* 1996 U.S.C.C.A.N. 4034, 4034–35, *available at* http://archives.clintonpresidentialcenter.org/?u=101196-remarks-by-president-on-economic-espionage-act-signing.htm.

> damage, or steal from computer networks. I am pleased to sign it into law.[22]

The EEA is a watershed statute, recognizing the national interest in protecting the trade secret assets of U.S. companies; but the EEA is ineffective as just a criminal statute; the EEA must be amended to add a private civil cause of action to protect the trade secret assets of U.S. companies.

II. PROPRIETARY INFORMATION LOSSES

ASIS International (ASIS) is the largest organization for security professionals with approximately 36,000 members worldwide.[23] ASIS has conducted 7 *Trends in Proprietary Information Loss Surveys* over the past 17 years.[24] "The resulting reports have been used by U.S. government agencies and private entities."[25] The ASIS survey is now considered the most authoritative resource on proprietary information losses by U.S. companies[26] and the survey findings are relied upon by and cited in the *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*.[27]

The ASIS Survey Report published in August 2007 was based upon a survey of a 144 respondents from a diverse array of U.S. businesses during the spring and summer of 2006.[28] The results confirm that proprietary information losses are continuing and increasing both in the United States and abroad.[29] U.S. companies continue to suffer major losses and 60% of the survey respondents with the requisite knowledge admitted that attempted or actual trade secret theft occurred in their respective companies in 2005.[30] Moreover, most of the information reported to have been compromised was physically located in the U.S. when the "compromise" occurred, but the major beneficiaries of the theft were foreign entities.[31] The top three foreign countries identified were China, Russia and India.[32] Deliberate and inadvertent actions of current and former employees; the exploitation of trusted third-party relationships (vendors, customers, joint ventures, subcontractors, outsourced providers); as well as "social engineering" and the unauthorized use of

---

[22] *Id.*

[23] ASIS International, About ASIS, http://www.asisonline.org/about/history/index.xml (last visited Aug. 29, 2008).

[24] ASIS INTERNATIONAL, TRENDS IN PROPRIETARY INFORMATION LOSS 4 (2007), *available at* http://www.asisonline.org/newsroom/surveys/spi2.pdf.

[25] *Id.*

[26] *Id.* at 1 (noting that the survey "has come to be recognized as the premier study of its kind").

[27] *Id.* at 4 (noting that the survey "findings have been cited in the *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*").

[28] *Id.* at 1.

[29] *Id.* at 11 ("Despite measures to ameliorate risk, U.S. companies continue to suffer losses").

[30] *Id.*

[31] *Id.*

[32] *Id.* at 24 (noting that "China, Russia, and India were identified as the top intended non-U.S. recipients of compromised information").

data mining software all contributed to proprietary information losses.[33] These losses ranged from less than $10,000 to more than $5.5 million.[34]

Former FBI Director Robert Mueller has testified that the ASIS estimate is grossly understated and has estimated that as much as $200 billion was lost by U.S. companies to economic espionage in 2002 alone.[35] Other sources claim the loss as high as $300 billion annually.[36] The threat is real, the consequences are significant, and the proposed EEA amendments in this article are absolutely necessary to address these serious issues.

III. FEDERAL PROTECTION OF INTELLECTUAL PROPERTY ASSETS

U.S. law protects patents, copyrights, trademarks and trade secrets.[37] There is a civil cause of action under federal law for patent infringement.[38] There is a civil cause of action under federal law for copyright infringement.[39] There is a civil cause of action under federal law for trademark infringement.[40] There is *not*, however, a civil cause of action under federal law for trade secret misappropriation.[41]

The reasons for the step-child treatment of trade secrets are historical.[42] Patents and trademarks are the by-products of the Industrial Revolution.[43]

---

[33] *Id.* at 3.

[34] *Id.*

[35] Robert Mueller, Dir., Fed. Bureau of Investigations, Address at the National Press Club Luncheon (June 20, 2003) ("Economic espionage is costing our U.S. businesses now more than $200 billion a year in the theft of intellectual property.").

[36] OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXECUTIVE, ANNUAL REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE – 2002 vii (2003), *available at* http://www.fas.org/irp/ops/ci/docs/2002.pdf ("[T]he combined costs of foreign and domestic economic espionage, including the theft of intellectual property, [may be] as high as $300 billion per year and rising."); Rustad, *supra* note 4, at 466–67; Richard Krantz, *Industrial Espionage Becomes Favorite Way to Achieve Quick Gains*, Voice of Am. News, April 29, 2005, http://www.voanews.com/english/archive/2005-04/2005-04-29-voa1.cfm ("The FBI's current estimate for 2004 is a loss of somewhere between $130 billion and $330 billion. We characterize around 15 or 16 countries as having pretty aggressive programs targeting the United States," says [FBI counterespionage official] Clayt Lemme.").

[37] Lanham Act, 15 U.S.C. §§ 1051–1072 (2006) (trademarks); Copyright Act, 17 U.S.C. §§ 101–122 (copyrights); Economic Espionage Act, 18 U.S.C. §§ 1831–1839 (trade secrets); Patent Act, 35 U.S.C. §§ 101–105, 161–164, 171–173 (patents).

[38] *See* 35 U.S.C. §§ 271–73.

[39] *See* 17 U.S.C. §§ 501–05.

[40] *See* 15 U.S.C. §§ 1114–17.

[41] *Compare id.*, 17 U.S.C. §§ 501–05, *and* 35 U.S.C. §§ 271–73, *with* 18 U.S.C. §§ 1831–39.

[42] *See* Katarzyna A. Czapracka, *Antitrust and Trade Secrets: The U.S. and the EU Approach,* 24 SANTA CLARA COMPUTER & HIGH TECH. L.J. 207, 213–14 (2008) ("Trade secret protection has been based on a number of different legal theories: contract, property, fiduciary relationship, and unjust enrichment. It is unclear whether trade secrets can be characterized as property rights in a manner imilar to copyrights or patents." (footnotes omitted)); Michael P. Simpson, Note, *Future of Innovation Trade Secrets, Property Rights, and Protectionism – an Age-Old Tale*, 70 BROOK. L. REV. 1121, 1140–44 (2005). Trade secret protection evolved from a property right into the prevention of unfair competition. *Id.* at 1140, 1142.

[43] *See* ANNE GILSON ET AL., GILSON ON TRADEMARKS § 1.03[3][a] (2008) (emphasizing the Industrial Revolution further distanced consumers from manufactures and products, thus stronger trademark protection was needed); Lawrence G. Kastriner, *The Revival of Confidence in the Patent*

Copyrights date back to the invention of the printing press, if not earlier.[44] Trade secrets were viewed at various times as unfair competition or quasi-contract rights with different labels attached to such rights in law and equity.[45]

Even though the protection of confidential information dates back to Roman law[46], and even though the birth of every patent starts out as a trade secret[47], the fact remains that trade secrets did not find a solid home in intellectual property law until the seminal decision in *Kewanee Oil Co. v. Bicron Corp.*[48] in 1974. Shortly thereafter, the Uniform Trade Secrets Act (UTSA) was promulgated by the National Conference of Commissioners on Uniform State Laws in 1979.[49] The stage was now set. In 1984, the United States Supreme Court in *Ruckelshaus v. Monsanto*[50] held that a trade secret asset was a property right protected by the United States Constitution.[51]

Of course, it should be noted that the transformation from the Industrial Revolution to the Information Age did not culminate until the advent of personal computers in the 1980s.[52] Since trade secrets are defined as commercially valuable

---

System, 73 J. PAT. & TRADEMARK OFF. SOC'Y 5, 6 (1991) (stating that U.S. patent protection was strengthened by the Industrial Revolution and laissez-faire economics); *see also* Lawrence M. Sung, Comment, *Intellectual Property Protection or Protectionalism? Declaratory Judgment Use by Patent Owners Against Prospective Infringers*, 42 AM. U.L. REV. 239, 245 n.35 (1992) (highlighting the Industrial Revolution's strengthening of patent protection).

[44] Sony Corp. of Am. v. Universal City Studios, Inc. 464 U.S. 417, 430 (1984).

[45] Milton E. Babirak, Jr., *The Maryland Uniform Trade Secret Act: A Critical Summary of the Act and Case Law*, 31 U. BALT. L. REV. 181, 183 (2002) (stating that since the late Middle Ages any trade secret protection was based on what would be considered as unfair competition); *see* Elizabeth A. Rowe, *Saving Trade Secret Disclosures on the Internet Through Sequential Preservation*, 2007 B.C. Intell. Prop. & Tech. F. 249, ¶ 18 (2007); Simpson, *supra* note 42, at 1142 (discussing trade secret law's evolution into something similar to contract law).

> Trade secret law is a branch of intellectual property law that most closely regulates standards of commercial ethics, guides morality of the business world, and underscores fair dealing. It is probably in part for this reason that trade secret law is now codified in the Restatement of Unfair Competition rather than in the Restatement of Torts.

Rowe, *supra*, at ¶18 (footnotes omitted).

[46] William B. Barton, *A Study in the Law of Trade Secrets*, 13 U. CIN. L. REV. 507, 507 (1939); Herbert David Klein, *The Technical Trade Secret Quadrangle: A Survey*, 55 NW. U. L. REV. 437, 437 (1960); A. Arthur Schiller, *Trade Secrets and the Roman Law: The Actio Servi Corrupti*, 30 COLUM. L. REV. 837, 837–38 (1930).

[47] James Pooley, *Fifty-Seventh Judicial Conference of the Third Circuit: Looking Forward to the Next Millenium: The Top Ten Issues in Trade Secret Law*, 70 TEMP. L. REV.1181, 1181 (1997).

[48] 416 U.S. 470 (1974).

[49] UNIF. TRADE SECRETS ACT, 14 U.L.A. 530 (2005).

[50] 467 U.S. 986 (1984).

[51] *Id.* at 1002 (stating that a government taking of a trade secrets is governed by the Fifth Amendment).

[52] M. Scott Boone, *The Past, Present, and Future of Computing and its Impact on Digital Rights Management*, 2008 MICH. ST. L. REV. 413, 413–27 (discussing the importance of personal computers by examining the implications of a world without personal computers); Paul Taylor, *Glory Days of IT's Midwife May be Over: Personal Computers*, WORLD ECON. AND FIN., Sept. 24, 1999, at 20 (emphasizing personal computers has been the most important change since the Industrial Revolution).

"information," it is not surprising that trade secrets have exploded onto the national scene.[53]

Nevertheless, it has been twelve years since the enactment of the EEA and the recognition that the protection of trade secrets is in the national and economic interest of the United States.[54] It is now out of step with the times to relegate U.S. companies to state statutes for protection of this important national intellectual property asset.

IV. PRIVATE ENFORCEMENT

U.S. businesses are the creators and owners of trade secret assets.[55] U.S. businesses are the victims of trade secret theft and foreign economic espionage.[56] U.S. businesses have the fiduciary and statutory obligation to protect trade secret assets; [57] finally, U.S. corporations have the financial means and financial incentive

---

[53] *See, e.g.*, BLAIR & WALLMAN, *supra* note 11 (explaining and evaluating the emerging importance of a business's intangible assets, including trade secrets); John Markoff, *Maker of Electric Cars Sues Rival Over Trade Secrets*, N.Y. TIMES, Apr. 15, 2008, at C5 (detailing the importance of a Tesla's Motors lawsuit against a competitor and its effect on the automobile industry); Scott Stewart, *At Work, Can You Keep What You A Trade Secret?*, ST. LOUIS POST–DISPATCH, Apr. 20, 2008, at E7 (discussing how companies can protect their trade secrets).

[54] H.R. REP. NO. 104–788, at 4 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4022–23 (stating because trade secrets are vital to America's economy, they need to be protected for both national economy and security reasons); 142 CONG. REC. S377 (1996) (statement of Sen. Cohen); *Id.* at H10,461 (statement of Rep. Hyde) ("In my opinion, our economic interests should be seen as an integral part of [the country's] national security interests, because America's standing in the world depends on its economic strength and productivity."); Jenifer Sawyer Klein, Note, *"I'm Your Therapist, You Can Tell Me Anything": The Supreme Court Confirms the Psychotherapist–Patient Privilege in* Jaffee v. Redmond, 47 DEPAUL L. REV. 701, 704 (1998) (stating that trade secrets are important to the economy and national security).

> While the cost of politico-military espionage was reduced military security, and damage from economic espionage comes in the form of billions of dollars annually in lost international contracts, pirated products and stolen corporate proprietary information. The direct cost of this espionage is borne by America's international corporations. The indirect costs are borne by the American economy as a whole – jobs and profits are lost; the competitive edge is stolen away.

142 CONG. REC. S377.

[55] *See* Stewart, *supra* note 53, at E7 (articulating that businesses put significant efforts into creating intellectual property but fail to put the same effort into protecting that intellectual property).

[56] 142 CONG. REC. S377 (1996) (statement of Sen. Cohen) ("The direct cost of this espionage is borne by America's international corporations."); *see, e.g., Engineer Who Tried to Sell Secrets to China Gets 24 Months*, CHI. TRIB., June 19, 2008, § 3, at 4 (reporting that a former employee of the U.S. company Quantum 3D Inc. tried to give trade secrets to the Chinese government and was sentenced to 24 months of jail under the EEA); Sean Webby, *Tech Spies Difficult to Catch: U.S. Espionage Law Fails to Nab Anyone After 5 Years with Silicon Valley at "Ground Zero," Authorities are Attempting to Stop the Flow of Business Trade Secrets Out of the Country*, SAN JOSE MERCURY NEWS (California), Feb. 11, 2001, at 1B (stating U.S. companies lost over $1 trillion in 2000 to foreign companies that misappropriated trade secrets).

[57] R. MARK HALLIGAN & RICHARD F. WEYAND, TRADE SECRET ASSET MANAGEMENT: AN EXECUTIVE'S GUIDE TO INFORMATION ASSET MANAGEMENT, INCLUDING SARBANES-OXLEY ACCOUNTING REQUIREMENTS FOR TRADE SECRETS 137–144 (2006.

to protect trade secret assets.[58] The legislative history of the EEA recognizes that the protection of trade secret assets is in the national interest of the United States.[59] Depriving U.S. companies from access to the federal courts under the EEA to protect trade secret assets is crippling U.S. companies in the New Economy.

V. THE EEA STATUTORY FRAMEWORK

The Economic Espionage Act is divided into two sections: Section 1831 (economic espionage by foreign governments, foreign instrumentalities or foreign agents) and Section 1832 (trade secret theft).[60] The proposed amendments to the EEA set forth in Appendix A will create a private cause of action under Section 1832; however there will be no amendments to the EEA relating to Section 1831 violations.[61]

A. Prohibited Acts

Both sections 1831 and 1832 of the EEA prohibit the same misconduct regarding trade secrets, punishing anyone who:

- "[S]teals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;"[62]
- "[W]ithout authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;"[63]
- "[R]eceives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization."[64]

The EEA does not prohibit legitimate means of obtaining information, such as reverse engineering or independent development.[65] Moreover, the EEA was not

---

[58] Czapracka, *supra* note 42, at 211 ("Trade secrets provide an economic incentive for private investment in knowledge production by giving the means to exclude others from using that knowledge and thus increasing the expected returns of innovation." (footnote omitted)); *see* Atkins, *supra* note 18, at 1174. Because a trade secret's value is diluted if a business does not actively protect it, a business will use reasonable means to protect its trade secrets. *Id.* at 1193–94.

[59] H.R. REP. NO. 104–788, at 4 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4022–23 (stating because trade secrets are vital to America's economy, they need to be protected for both national economy and security reasons); 142 CONG. REC. H10,461 (1996) (statement of Rep. Hyde) ("In my opinion, our economic interests should be seen as an integral part of [the country's] national security interests, because America's standing in the world depends on its economic strength and productivity.").

[60] 18 U.S.C. § 1831 (2006) (entitled "Economic Espionage"); *id.* § 1832 (entitled "Theft of Trade Secrets").

[61] *See infra* Appendix A.

[62] 18 U.S.C. § 1832(a)(1); *accord id.* § 1831(a)(1).

[63] 18 U.S.C. § 1832(a)(2); *accord id.* § 1831(a)(2).

[64] 18 U.S.C. § 1832(a)(3); *accord id.* § 1831(a)(3).

[65] *See* 142 CONG. REC. S12,213 (1996) (Manager's Statement for H.R. 3723, The Economic Espionage Bill) ("If someone has lawfully gained access to a trade secret and can replicate it without

intended to deny an employee the inherent right to use of general knowledge, skills, or experience derived from his or her tenure with a particular company.[66]

The EEA also makes it a federal offense to receive, buy or possess the trade secret information of another person knowing that such information was stolen, appropriated, obtained or converted without the trade secret owner's authorization.[67]

The EEA's definition of "trade secret" is derived from the Uniform Trade Secrets Act ("UTSA") but has been updated to reflect the realities of the electronic environment where proprietary information assets now often exist:

> [T]he term "trade secret" means all forms and types on financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if --
>
> (A) the owner thereof has taken reasonable measures to keep such information secret; and
>
> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.[68]

Conspiracies and attempted thefts are also proscribed by the EEA.[69] The same types of penalties apply with increased penalties imposed if the trade secret

---

violating copyright, patent or [the EEA], then that form of 'reverse engineering' should be fine."). Independent, or parallel creation, is not prohibited by the EEA. *Id.* at S12,212; *Id.* at S10,886 (statement of Sen. Kohl) ("Reverse engineering is a broad term that encompasses a variery of actions. The important thing is to focus on whether the accused committed one of the prohibited acts of this statute rather than whether he or she has 'reverse engineered.'"); *Id.* at H10,462 (statement of Rep. Schumer) ("[R]everse engineering is an entirely legitimate practice."). *But see* James H.A. Pooley, Mark A. Lemley, & Peter J. Toren, *Understanding the Economic Espionage Act of 1996 ,* 5 TEX. INTELL. PROP. L.J. 177, 195 (1997) ("While reverse engineering is not expressly prohibited under [18 U.S.C. § 1831(a)(2)], neither is it expressly permitted."). The EEA does not expressly state reverse engineering is allowed. Pooley, Lemley, & Toren, *supra*, at 195. Therefore, some forms of reverse engineering may be prohibited if the acts involved are unlawful under the EEA. *Id.*; *see also* Darren S. Tucker, Comment, *The Federal Government's War on Economic Espionage*, 18 U. PA. J. INT'L ECON. L. 1109, 1143 (1997) (discussing whether reverse engineering and independent creation is allowed under EEA).

[66] *See*, 142 CONG. REC. S12,213 (1996) (Manager's Statement for H.R. 3723, The Economic Espionage Bill) ("[T]he government cannot prosecute an individual for taking advantage of the general knowledge and skills or experience that he or she obtains or comes by during his tenure with a company."); *id.* at H10,462 (statement of Rep. Schumer) ("[S]ome Members thought that this legislation might inhibit common and acceptable business practices. For example, employees who leave one company to work for another naturally take their general knowledge and experience with them and no one, no one wishes to see them penalized as a result."); *see also* Tucker, *supra* note 65, at 1143.

[67] 18 U.S.C. § 1831(a)(3); *id.* § 1832(a)(3).

[68] 18 U.S.C. § 1839(3). *Compare id.* (defining "trade secret" under the EEA), *with* UNIF. TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 538 (2005) (defining "trade secret" under the UTSA).

misappropriation benefits a foreign government, foreign instrumentality or foreign agent.[70]

The EEA also provides for forfeiture to the United States of any property constituting or derived from the proceeds of violations of the act and the forfeiture of any property used or intended to be used, in any manner or part, to commit or facilitate a violation of the act.[71]

The EEA authorizes the attorney general, deputy attorney general or assistant attorney general in the Criminal Division of the Justice Department to apply for a federal court order authorizing or approving the interception of wire or oral communications by the FBI or other federal agencies having responsibility for the investigation of the offense.[72] These are the same investigative tools available in other federal criminal prosecutions.[73]

The EEA also applies to offenses committed outside the United States if the offender is a citizen or permanent resident alien of the United States, if the corporation or other organization was incorporated or organized in the United States, or if an act in furtherance of the offense was committed in the United States.[74] These extraterritorial provisions are critical to deter international theft and to prevent willful evasion of liability for trade secret misappropriation by using the Internet or other means to transfer the proprietary information outside the United States.

In any prosecution or other proceeding under the EEA, the court is required to issue protective orders and to take such other action necessary to preserve the confidentiality of the trade secrets consistent with the federal rules of criminal and civil procedure.[75] The attorney general is authorized to commence civil actions to obtain injunctive relief to protect the trade secret owner from any violations or further violations of the act.[76]

The EEA does not displace any other remedies, civil or criminal, relating to the misappropriation or theft of trade secrets or the lawful disclosure of information required by law or necessary actions by a government entity of the United States, a state or political subdivision or a state.[77]

---

[69] 18 U.S.C. § 1831(a)(5); *id.* § 1832(a)(5).

[70] 18 U.S.C. § 1831(a). *Compare id.* (providing a maximum penalty of a fine and 15 years imprisonment), *with id.* § 1832(a) (providing a maximum penalty of a fine and 10 years imprisonment).

[71] 18 U.S.C. § 1834(a).

[72] *Id.* § 2516(1)(a).

[73] *Id.* (providing for interception of wire or oral communications for a myriad of federal crimes); *see generally* 28 U.S.C. § 533 (discussing the U.S. Attorney General's power to appoint officials to conduct and carry out investigations).

[74] 18 U.S.C. § 1837.

[75] *Id.* § 1835; 142 CONG. REC. H10,461 (1996) (Statement of Rep. Buyer).

> Another obstacle to enforcing these crimes under existing law is that there is no statutory procedure in place to protect the victim's stolen information during criminal proceedings. As a result, victims are often reluctant to prosecute for fear that the prosecution itself will further disseminate the economic information stolen from them.

Id.

[76] *Id.* § 1836.

[77] *Id.* § 1838.

VI. PROSECUTIONS UNDER THE EEA

Since the enactment of the EEA, there have been less than sixty prosecutions, mainly section 1832 prosecutions.[78] Most of these prosecutions were filed in the Northern District of California.[79] In fact, Justice Department statistics confirm that approximately 80% of the eighty six federal judicial districts nationwide have had no EEA prosecutions.[80]

VII. NO PREEMPTION

The proposed amendments to the EEA set forth in Appendix A will not preempt either the UTSA or the common law.[81] The law of trade secrets has developed over many centuries and should not be displaced.[82] Likewise, the UTSA will still often be the statutory cause of action of choice in cases where federal jurisdiction is not necessary or warranted.[83] Such an approach is followed in trademark law.[84] The federal trademark statute (Lanham Act) does not preempt the common law or state causes of action for trademark infringement.[85]

VIII. NATIONAL SERVICE OF PROCESS

The federal courts provide for national service of process.[86] This procedural advantage is critical in trade secrets litigation. Often the plaintiff resides in one state; the defendant resides in another; and the evidence of misappropriation and critical witnesses are in different states around the country.[87]

Faced with this situation, a skilled trade secrets practitioner looks for a way to bring the case in federal court so he can serve nationwide subpoenas and proceed

---

[78] Susan W. Brenner & Anthony C. Crescenzi, *State Sponsored Crime: The Futility of the Economic Espionage Act*, 28 HOUS. J. INT'L L. 389, 432 (2006) (stating that as of 2006, there have been forty-seven people prosecuted in thirty-four cases under the Economic Espionage Act).

[79] *See* Computer Crime & Intellectual Property Section, U.S. Dep't of Justice, Trade Secret/Economic Espionage Cases, http://www.usdoj.gov./criminal/cybercrime/ipcases.html#eea (showing that many of the recent U.S. Department of Justice Economic Espionage Act prosecutions are in the Northern District of California).

[80] *See Id.* (listing only sixteen different federal circuit courts handling cases involving the EEA).

[81] *See infra* Appendix A.

[82] 1 MELVIN. F. JAGER, TRADE SECRETS LAW § 1:3 (2008) (discussing how the concept of protecting trade secrets can be traced back to the ancient Romans).

[83] UNIF. TRADE SECRETS ACT § 7(a) (amended 1985), 14 U.L.A. 651 (2005).

[84] Anne Hiaring, *Basic Principles of Trademark Law*, *in* UNDERSTANDING TRADEMARK LAW 2008, at 51, 56–57 (PLI Patents, Copyrights, Trademarks, & Literary Prop., Course Handbook Series No. 939, 2008).

[85] Kardex Sys., Inc. v. Sistemco N.V., 583 F.Supp. 803, 810 n.3 (D. Me. 1984) ("The Lanham Act does not preempt state efforts to establish and protect rights in trademarks.").

[86] 28 U.S.C. § 1391 (2006) (providing for national service of process in all civil actions).

[87] *See, e.g.*, Pepsico, Inc. v. Redmond, 54 F.3d 1262, 1264 (7th Cir. 1995).

with discovery anywhere in the country.[88] But securing federal jurisdiction is difficult. Unless there is diversity of citizenship under 28 U.S.C. § 1332, there is no way to obtain subject matter jurisdiction to the federal courts without a federal cause of action (28 U.S.C. § 1331) and pendent jurisdiction of the state-based trade secret claims pursuant to 28 U.S.C. § 1367.[89] This explains why trade secret litigators are now filing federal Computer Fraud and Abuse Act ("CFAA") claims which establish subject matter jurisdiction in federal court and provide jurisdiction for related trade secret claims pursuant to the supplemental jurisdiction of the federal courts.[90]

The difficulties in litigating a national trade secrets dispute under a state-based statute cannot be overemphasized. Take a simple example: suppose the trade secrets case is pending in state court in Illinois and discovery establishes that a critical witness with potentially smoking-gun evidence resides in California. The first step required is the filing of a motion in Illinois state court requesting the Illinois court to issue a discovery petition authorizing the out-of-state deposition.[91] After obtaining the Illinois court order, a special action must then be filed in California to obtain a court order from the California court under the doctrine of comity among states to authorize the valid issuance of the subpoena in California to the California resident.[92] The whole process can take months with briefings both in the Illinois courts and the California courts.[93]

Amending the EEA to add a private civil cause of action will instantly eliminate all these procedural hurdles and delays. Subpoenas can be issued nationwide by trial counsel in federal court litigation.[94] Trade secret cases are time sensitive – "[a] trade secret once lost is, of course, lost forever".[95] This procedural advantage alone, *without more*, merits the amendments to the EEA set forth in Appendix A of this article.

---

[88] *See* Roy E. Hofer & Susan F. Gullotti, *Presenting the Trade Secret Owner's Case*, *in* PROTECTING TRADE SECRETS 1985, at 145, 160–61 (PLI Patents, Copyrights, Trademarks, & Literary Prop., Course Handbook Series No. 196, 1985).

[89] *Id.* at 159–60.

[90] Victoria A. Cundiff, *Protecting Trade Secrets in a Digital World*, *in* INFORMATION TECHNOLOGY LAW INSTITUTE 2008: NEW DIRECTIONS: SOCIAL NETWORKS, BLOGS, PRIVACY, MASH-UPS, VIRTUAL WORLDS AND OPEN SOURCE, at 723, 731–32 (PLI Patents, Copyrights, Trademarks, & Literary Prop., Course Handbook Series No. 929, 2008).

[91] ILL. SUP. CT. R. 201(o).

[92] U.S. DIST. CT. E.D. CAL. R. 30-250(a).

[93] Mark C. Dillon, *Obtaining Out-of-State Witnesses and Documents for Discovery and Trial*, 28 WESTCHESTER B.J. 13, 14 (2001) (noting that practitioners are at the mercy of foreign courts in these matters).

[94] Franklin E. Fink, *The Name Behind the Screenname: Handling Information Requests Relating to Electronic Communications*, *in* SEVENTH ANNUAL INTERNET LAW INSTITUTE, at 953, 972–73 (PLI Patents, Copyrights, Trademarks, & Literary Prop., Course Handbook Series No. 754, 2003).

[95] FMC Corp. v. Taiwan Tainan Giant Indus. Co., Ltd., 730 F.2d 61, 63 (2d Cir. 1984).

IX. *EX PARTE* SEIZURE ORDERS

Another advantage of the proposed EEA amendments would be the statutory recognition of civil *ex parte* orders in trade secret misappropriation lawsuits.[96] Once again, in today's environment, trade secrets can be transferred to foreign countries and other parts of the world in seconds.[97] The traditional process of notice to the defendant and opportunity to be heard do *not* work well in trade secret cases because the defendants can hide or destroy the purloined trade secret assets in seconds.[98] To preserve the status quo and to preserve the evidence, courts must have clear statutory authority to issue *ex parte* seizure orders in trade secret cases and the proposed amendment to the EEA set forth in Appendix A includes this provision as new subsection (c) in section 1834 of the EEA.[99]

X. EXTRATERRITORIAL JURISDICTION

Because trade secret assets can be stolen and transferred anywhere in the world, the trade secret owner needs the protection of the United States Constitution to the fullest extent possible.[100] The Congress of the United States recognized this with the passage of the EEA and provided for extraterritorial jurisdiction to encompass misconduct occurring outside the United States within the outer limits of the U.S. Constitution[101] reigning in (1) offenders committing wrongful acts outside the United States if they are citizens, permanent resident aliens, or entities organized under the law of the United States[102] and (2) wrongful conduct if any acts in furtherance of the offense occurred in the United States.[103]

The proposed amendments to the EEA would extend the benefits of extraterritorial jurisdiction to EEA civil actions which, in turn, will provide significant new protection against the rampant economic espionage attacks directed toward U.S. companies.[104]

---

[96] *See infra* Appendix A.

[97] Cameron R. Graham & Matt Zinn, *Cable On-Line Services*, *in* CABLE TELEVISION LAW 2000, at 769, 829–30 (PLI Patents, Copyrights, Trademarks, & Literary Prop., Course Handbook Series No. 593, 2000).

[98] *See id.*; *see also* Elizabeth A. Rowe, *Saving Trade Secret Disclosures on the Internet Through Sequential Preservation*, 42 WAKE FOREST L. REV. 1, 3–4 (2007) (noting that the power of the Internet exponentially magnifies the risk of trade secret disclosure).

[99] *See infra* Appendix A.

[100] *See* Ian C. Ballon, *The Economic Espionage Act of 1996*, *in* 17TH ANNUAL INSTITUTE ON COMPUTER LAW: THE EVOLVING LAW OF THE INTERNET-COMMERCE, FREE SPEECH, SECURITY, OBSENITY AND ENTERTAINMENT, at 755, 760–61 (PLI Patents, Copyrights, Trademarks, & Literary Prop., Course Handbook Series No. 471, 1997).

[101] *Id.* at 761–62.

[102] 18 U.S.C. § 1837(1) (2006); Ballon, *supra* note 100, at 761–62.

[103] 18 U.S.C. § 1837(2); Ballon, *supra* note 100, at 761–62.

[104] *See infra* Appendix A.

XI. UNIFORMITY

There has been much discussion regarding the lack of uniformity in state trade secret laws.[105] This author does not share this view; the UTSA has, for the most part, resulted in a very coherent and consistent body of trade secrets law – what constitutes a "trade secret" is now defined by statute;[106] what constitutes "misappropriation" is now defined by statute;[107] there is a uniform statute of limitations;[108] statutory standards for injunctive relief;[109] statutory provisions for compensatory damages[110] and so on.[111]

However, there are still some glaring holes and discrepancies.[112] New York, for example, has never enacted the UTSA.[113] New Jersey, Massachusetts and Texas have not enacted the UTSA either.[114] There are other state variances requiring U.S. courts to address choice of law questions in most national trade secret cases.[115] Adding a private cause of action to the EEA will provide the courts with the opportunity to develop a more uniform approach to trade secrets derived from the unique national and international perspective of the federal courts. U.S. companies now compete in a global marketplace; a national and international perspective is now required for the protection of trade secret assets.[116]

---

[105] *E.g.*, Christopher Rebel J. Pace, *The Case for A Federal Trade Secrets Act*, 8 Harv. J. Law & Tech. 427, 442 (1995) ("The best reason enacting federal legislation to displace state law on trade secret misappropriation is the need for national uniformity in this area of law."); 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, 801 (1999).

[106] UNIF. TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 538 (2005).

[107] *Id.* § 1(2).

[108] *Id.* § 6.

[109] *Id.* § 2.

[110] *Id.* § 3.

[111] *See id.* §§ 1–12.

[112] *See* Pace, *supra* note 105, at 442–43 ("[E]very state protects a business' trade secrets from misappropriation, and the vast majority do so via the adoption of state statutes based on the UTSA. Yet, despite this universal recognition and near-universal origin of trade secrets protection, states vary widely in their treatment of trade secret misappropriation."). The UTSA has been adopted by forty-five states, the District of Columbia, and the U.S. Virgin Islands. 14 U.L.A. at 18–19 (Supp. 2008); *see* Julie Piper, Comment, *I Have A Secret?: Applying the Uniform Trade Secrets Act to Confidential Information that does not Rise to the Level of Trade Secret Status*, 12 MARQ. INTELL. PROP. L. REV. 359, 360 (2008) (discussing the history and development of trade secret law as interpreted and adopted by different states).

[113] Michael J. Hutter, *The Case for Adoption of a Uniform Trade Secrets Act in New York*, 10 ALB. L.J. SCI. & TECH. 1, 6–8 (1999) (noting the advantages for New York enacting the USTA); Pace, *supra* note 105, at 443 (noting that New York continues to prefer the Restatement approach to trade secret misappropriation).

[114] *See* Hutter, *supra* note 113, at 6–8; Pace, *supra* note 105, at 443.

[115] Allyson A. McKenzie, United States v. Kai-Lo Hsu*: An Examination of the Confidentiality Provision in the Economic Espionage Act: Is it Suitable to Maintain the Use and Effectiveness of the EEA?*, 25 DEL. J. CORP. L. 309, 314 (2000) (noting that different laws among the states create choice of law questions).

[116] 142 CONG. REC. S740 (1996) (statement of Sen. Kohl) ("It would not be unfair to say that America has become a full-service shopping mall for foreign governments and companies who want to jump start their businesses with stolen trade secrets."); *Id.* at S377 (statement of Sen. Cohen); MELVIN F. JAGER, TRADE SECRETS THROUGHOUT THE WORLD (Thomson/West 2007) (detailing the various trade secret rules and laws in effect the world over).

XII. INTERNATIONAL TRADE AND TREATY OBLIGATIONS

The United States has entered into numerous international agreements and many of these agreements require the member countries to protect intellectual property rights.[117]

The two most significant examples of this trend are the North American Free Trade Agreement ("NAFTA")[118] and the Agreement Establishing World Trade Organization ("WTO") which resulted from the Uruguay Round Talks under the General Agreement on Tariffs and Trade ("GATT") and the WTO/GATT Agreement entitled Trade-Related Aspects of Intellectual Property Rights ("TRIPS").[119]

Both NAFTA and the TRIPS Agreement require national standards for trade secret protection.[120] However the United States has not enacted a federal statute to protect trade secrets; states like New York, Massachusetts, Texas do not even have a state trade secrets statute.[121] So the prevailing argument in the international community goes something like this: if the United States does not have a federal civil statute to protect trade secrets, why should we be held to a higher standard in our respective countries?[122] This argument is well taken; although the US recognized the important national interest in the protection of trade secret assets with the passage of the EEA in 1996; we are long overdue for the enactment of a federal trade secrets statute. These goals can be accomplished quickly and efficiently by enacting the proposed amendments set forth in Appendix A.

> While the cost of politico-military espionage was reduced military security, and damage from economic espionage comes in the form of billions of dollars annually in lost international contracts, pirated products and stolen corporate proprietary information. The direct cost of this espionage is borne by America's international corporations. The indirect costs are borne by the American economy as a whole – jobs and profits are lost; the competitive edge is stolen away.

142 CONG. REC. S377.

[117] *See* Michael W. Carroll, *One For All: The Problem of Uniformity Cost in Intellectual Property Law*, 55 AM. U. L. REV. 845, 863 n.67 (2006) (listing various examples, including the Paris Convention for the Protection of Industrial Property, the Patent Cooperation Treaty, and the Berne Convention for the Protection of Literary and Artistic Works); Pace, *supra* note 105, at 450–453; Spencer Weber Waller & Noel J. Byrne, *Changing View of Intellectual Property and Competition Law in the European Community and the United States of America*, 20 BROOK. J. INT'L L. 1, 8 (1993).

[118] North American Free Trade Agreement, U.S.-Can.-Mex., Dec. 17, 1992, 32 I.L.M. 289 (1993) [hereinafter NAFTA]; Pace, *supra* note 105, at 450.

[119] Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, Legal Instruments – Results of the Uruguay Round of Multilateral Trade Negotiations 365, 1869 U.N.T.S. 299, 33 I.L.M 1197 [hereinafter TRIPs]; *see* Pace, *supra* note 105, at 450.

[120] TRIPs, *supra* note 119; NAFTA, *supra* note 118; *see* Pace, *supra* note 105, at 450.

[121] *See* McKenzie, *supra* note 115 at 314; Pace, *supra* note 105, at 443, 451–52.

[122] *See* Rustad, *supra* note 4, at 477 ("In general, the United States receives very little cooperation from our allies in prosecuting foreign spies.").

XIII. MORE EFFECTIVE PROTECTION OF TRADE SECRET ASSETS

There were many fears when the EEA was enacted.[123] A major concern was that aggressive business competition would be exposed to EEA criminal indictment.[124] This has not happened.[125] The EEA is a well-drafted statute with built-in safeguards that prevent abuse. There is also strong legislative history surrounding the EEA that alleviates such concerns.[126] EEA prosecutions have been targeted only to egregious and "open-and-shut" cases.[127] Most indictments involve "offers to sell" or "offers to buy" purloined trade secrets.[128]

---

[123] Robert C. Van Arnam, *Business War: Economic Espionage in the United States and the European Union and the Need for Greater Trade Secret Protection*, 27 N.C. J. INT'L L. & COM. REG. 95, 112 n.124 (2001); Leslie G. Berkowitz, *The Economics Espionage Act of 1996: An Experiment in Unintended Consequences?*, COLO. LAW., Dec. 1997, at 47, 49 (1997).

> Private sector impediments [to the effectiveness of the EEA] 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 the company's products.

Id.

[124] 142 CONG. REC. H10,462 (1996) (statement of Rep. Schumer) ("Our bill was carefully drafted to avoid this problem [of inhibiting common and acceptable business practices]. The very high intent requirements and the narrow definition of a trade secret make it clear that we are talking about extraordinary theft, not mere competition."); *see also* James M. Fischer, Note, *An Analysis of the Economic Espionage Act of 1996*, 25 SETON HALL LEGIS. J. 239 (2001) (discussing concerns surrounding this legislation).

[125] *See* Brenner & Crescenzi, *supra* note 78, at 433 n.184 (noting the number of prosecutions under the EEA is small compared to other intellectual property violations).

[126] 142 CONG. REC. H10,462 (1996) (statement of Rep. Schumer).

> First, some Members thought that this legislation might inhibit common and acceptable business practices. For example, employees leave one company for another to work for another naturally take their general knowledge and experience with them and no, no one wishes to see them penalized as a result. Similarly, reverse engineering is an entirely legitimate practice.
>
> Our bill was carefully drafted to avoid this problem. The very high intent requirements and the narrow definition of a trade secret make it clear that we are talking about extraordinary theft, not mere competition.
>
> Second, several Members were concerned that people acting in the public interest as whistleblowers would be subject to the penalties in this bill.
>
> Again, we have carefully fine-tuned the language to avoid this problem. . . . In other words, we are talking about thieves, not whistleblowers, and the legislation makes that clear.

Id.

[127] Van Arnam, *supra* note 123, at 112 (noting that the success of EEA prosecutions may be a result of the Department of Justice selecting cases it can win); *see also* Joseph N. Hosteny, *The Economic Espionage Act: A Very Mixed Blessing*, INTELL. PROP. TODAY, Feb. 1998, at 8, 10 (addressing the pros and cons of the EEA).

[128] *See generally* Hosteny, *supra* note 127, at 10 ("Cases brought thus far under the Economic Espionage Act appear consistent with the notion that egregious criminal activity will be required to justify a prosecution, and that foreign involvement enhances the chances of prosecution. All cases brought thus far comprise incidents of outright bribery and payments for tangible property."); Rowe, *supra* note 98, at 1–5 (discussing an example of employees misappropriating trade secrets and attempting to sell them on the Internet).

But therein lies the shortcoming of the EEA. Since September 11, 2001, the Justice Department and the FBI have been swamped with new priorities and new threats.[129] Trade secrets thefts are no longer a high priority.[130] The perception exists that these are business crimes that U.S. companies can litigate in the civil courts.[131] Not so. Trade secret claims *cannot* be litigated in federal court. There is no civil federal trade secrets statute, and subject matter jurisdiction in the federal courts is often non-existent.[132]

At the present time, multi-national U.S. corporations are faced with the dilemma that major trade secret theft cases are within the "prosecutorial discretion" of the Justice Department under the EEA[133] or limited to the vagaries and procedural disadvantages of state court litigation.[134] Neither option is satisfactory. The amendments to the EEA set forth in Appendix A would provide U.S. corporations with the full benefits of the EEA and balance the playing field in multi-national competition.

XIV. COMPARISONS TO THE COMPUTER FRAUD AND ABUSE ACT

The CFAA provides an excellent model to illustrate the advantages of adding a private civil cause of action to the EEA.[135] Like the EEA, the CFAA is a criminal statute.[136] The difference: the CFAA provides a civil cause of action: "Any person who suffers damage or loss may maintain a civil action against the violator...".[137]

Since most trade secrets now reside in an electronic environment, it is not surprising to see an upsurge in CFAA actions.[138] Today, "employers…are increasingly taking advantage of the CFAA's civil remedies to sue former employees

---

[129] *Comm. on House Judiciary Subcomm. on Commercial and Admin. Law* (Apr. 26, 2006) (statement of Michael A. Battle, Director of Executive Office for United States Attorneys), *available at* 2006 WLNR 7081736 (noting that the prosecution of terrorism since 9/11 continues to be the top priority of every U.S. attorney).

[130] Rustad, *supra* note 4, at 479 n.119. *See* Hosteny, *supra* note 127, at 9 (stating "the EEA is going to be selectively applied, at least for some time to come"). In many cases, the government only brings cases where a defendant's criminal intent and knowledge are clear so that there is a high probability of conviction. *Id.*

[131] Hosteny, *supra* note 127, at 8.

[132] Marina Lao, *Federalizing Trade Secrets Law in an Information Society*, 59 OHIO ST. L.J. 1633, 1635 (1998) (noting that trade secrets are regulated differently according to jurisdiction).

[133] Hosteny, *supra* note 127, at 10.

[134] McKenzie, *supra* note 115, at 314–15 (noting that state trade secrets laws do not fill the gap that federal laws leave open).

[135] *See* 18 U.S.C. § 1030 (2006).

[136] *Id.* § 1030(c) (setting forth punishments ranging from a fine to up to 20 years of imprisonment).

[137] *Id.* § 1030(g). Causes of action can be maintained for compensatory damages or equitable relief, such as an injunction. *Id.*

[138] Leslie G. Berkowitz, *Computer Security and Privacy: The Third Wave of Property Law*, COLO. LAW., February 2004, at 57, 59 (addressing the problems facing the information property wave); Linda K. Stevens & Jesi J. Carlson, *The CFAA: New Remedies for Employee Computer Abuse*, 96 ILL. B.J. 144, 144–45 (2008) (pointing out the increased number of law suits brought under the Computer Fraud and Abuse Act).

and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system."[139]

Section 1030(a) of the CFAA enumerates various categories of misconduct but the cases involving departing employees focus on the element of "without authorization" or "exceeding authorized access."[140] Recent cases have recognized that the CFAA provides a remedy against disloyal employees who download, transfer or delete trade secret information on company computers and who engage in other acts of trade secret misappropriation involving computers.[141]

The seminal decisions in *Shurgard Storage Centers, Inc. v. Safeguard Self-Storage, Inc.*[142] and *International Airport Centers, L.L.C. v. Citrin*[143] illustrate the use of the CFAA to combat trade secret misappropriation and to provide access to the U.S. federal courts.[144]

In *Shurgard*, employees accessed plaintiff's computer to transmit trade secrets to the new employer.[145] The district court rejected the argument that these employees had authorized access to *Shurgard's* computer system because they were still employed at *Shurgard*.[146] Instead, the court held that these employees lost their authorization and were "without authorization" when they accessed the *Shurgard's* computer system to send proprietary information via email to their new employer.[147]

In *International Airport Centers* v. *Citrin*, the reasoning in *Shurgard* was buttressed in an opinion by Judge Posner writing for the Seventh Circuit Court of Appeals.[148] Once again, the facts involved a disloyal employee who decided to quit and start up his own competing business.[149] Before he quit, however, *Citrin* deleted all the data that he had collected on potential acquisition targets for the benefit of IAC.[150] The issue was whether such pre-termination activities violated the CFAA because *Citrin* was authorized to use the laptop computer.[151] The Seventh Circuit made short shrift of this argument, holding that *Citrin's* authorization to access the company-issued laptop computer terminated when he breached his duty of loyalty to his former employer.[152]

However, the CFAA is *not* a federal trade secrets statute. The CFAA is primarily aimed at computer crimes, and the CFAA only has relevance to trade secret misappropriation claims when the trade secret theft coincides with computer

---

[139] Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003).

[140] *See* United States v. Phillips, 477 F.3d 215 (5th Cir. 2007); *see also* Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962 (D. Ariz. 2008).

[141] Garelli Wong & Assocs., Inc. v. Nichols, 551 F. Supp. 2d 704 (N.D. Ill. 2008) (granting employee's motion to dismiss because employer failed to allege damage under the CFAA).

[142] 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

[143] 440 F.3d 418 (7th Cir. 2006).

[144] *Id.*; *Shurgard*, 119 F. Supp. 2d at 1121.

[145] *Shurgard*, 119 F. Supp. 2d at 1123. The trade secrets at issue included plans for the development of a system for maximizing growth in the self-service storage facility industry. *Id.*

[146] *Id.* at 1129 (denying defendant's motion to dismiss).

[147] *Id.*

[148] *Citrin*, 440 F.3d 418.

[149] *Id.* at 419. The trade secrets at issue were data collected that identified potential acquisition targets in the real estate industry. *Id.*

[150] *Id.*

[151] *Id.* at 420.

[152] *Id.* at 421.

misuse.[153] Courts have been reluctant to transform the CFAA into a surrogate federal trade secret statute, and there have been numerous cases litigating the scope of the CFAA in recent years.[154]

Federal jurisdiction cannot rest entirely on the CFAA in complex trade secrets litigation. Instead, a federal trade secret statute is required. The solution is to enact, as soon as possible, the EEA amendments recommended in this article.

XV. OTHER ADVANTAGES OF AN EEA CIVIL CAUSE OF ACTION

Adding a private cause of action to the EEA will eliminate many of the barriers that now exist to the full realization of the benefits of the EEA.

The primary obstacle is the high burden of proof to obtain a criminal conviction requiring proof beyond a reasonable doubt.[155] Prosecutors want to proceed only with indictments they know will result in a conviction or plea agreement -- often requiring wiretap or video evidence to secure convictions.[156]

Invocation of the Fifth Amendment privilege against self-incrimination also hampers EEA prosecutions.[157] This is not an advantageous option in a civil suit since the invocation of the Fifth Amendment in a civil proceeding will result in a default judgment for the Plaintiff.[158]

Finally, adding a civil cause of action to the EEA will lower the burden of proof standard to the "preponderance of the evidence".[159] This is the same burden of proof standard for UTSA actions in state court.[160] The result will be more actions by U.S. companies to protect corporate trade secret assets benefiting the shareholders of U.S. companies as well as the U.S. economy.

---

[153] Linda K. Stevens & Jesi J. Carlson, *The CFAA: New Remedies for Employee Computer Abuse*, 96 ILL. B.J. 144, 145–46 (2008) (describing the damage departing employees have done using their previous employer's computer infrastructure).

[154] *Id.* (analyzing the way different courts have interpreted the CFAA).

[155] Rustad, *supra* note 4, at 522; Mondaq Bus. Briefing, *Restrictive Covenants and Trade Secrets Frequently Asked Questions on United States*, July 12, 2006, *available at* 2006 WLNR 16881363.

[156] Hosteny, *supra* note 127, at 9–10; *see* Rustad, *supra* note 4, at 458.

> The data on EEA defendant characteristics, targeted companies, the nature of trade secrets stolen, the method of misappropriation, and trends in cases prosecuted, reveals that the federal criminal statute is not punishing and deterring state-sponsored espionage. EEA prosecutors focus on domestic trade secret theft rather than foreign government involvement in industrial and economic espionage. Cybercriminals and other trade secret misappropriators are unlikely to be deterred with such a dismal record of detection and punishment of economic espionage by federal law enforcement.

Id.

[157] Joseph C. Bodiford, *"White-Collar" Crimes*, *in* BUSINESS LITIGATION IN FLORIDA §22.25 (2007) (examining one's right against self-incrimination in business crimes); Hosteny, *supra* note 127, at 10.

[158] Bodiford, *supra* note 157, at §22.25.

[159] Gerald J. Mossinghoff, J. Derek Mason, & David A. Oblon, *The Economic Espionage Act: A New Federal Regime of Trade Secret Protection*, 79 J. PAT. & TRADEMARK OFF. SOC'Y 191, 202 (1997).

[160] UNIF. TRADE SECRETS ACT §§ 1–12 (amended 1985), 14 U.L.A. 537–659 (2005).

CONCLUSION

In the new economy, in the Information Age, and in the international arena of global competition, the protection of trade secret assets of U.S. companies is now paramount. The enactment of the Economic Espionage Act of 1996 recognized that the protection of trade secret assets is in the national economic interest of the United States. There exist federal civil statutes to protect patents, copyrights and trademarks but there is no federal civil statute to protect trade secrets. The proposed amendments to the EEA set forth in Appendix A are simple and straightforward. The benefits will be substantial and immediate: (1) increased deterrence of economic espionage and trade secret theft; and (2) increased economic vitality of U.S. corporations both domestically and abroad.

APPENDIX A

PROPOSED AMENDMENTS TO THE ECONOMIC ESPIONAGE ACT TO ADD A CIVIL CAUSE OF ACTION FOR TRADE SECRET THEFT

§ 1831. Economic espionage

(a) In general. -- Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly --

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

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

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

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

(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of conspiracy,

shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.

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

§ 1832. Theft of trade secrets

(a) Whoever, with the intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly --

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;
(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

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

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

(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

(b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000.

(c) Civil remedies

(1) In general - Any person aggrieved by reason of conduct prohibited under subsection (a) of section 1832 may commence a civil action for relief set forth in subsection (2) of this section, subsection (3) of this section, and section 1836.

(2) In addition or in lieu of injunctive relief, a person who suffers damage or loss by reason of a violation of section 1832 may recover damages for actual loss caused by misappropriation. Such person may also recover for the unjust enrichment caused by misappropriation that is not taken into account in computing damages for actual loss.

(3) If willful or malicious misappropriation exists, the court may award exemplary damages in an amount not exceeding twice any award made under subsection (2).

§ 1833. Exceptions to prohibitions

This chapter does not prohibit --

(1) any otherwise lawful activity conducted by a governmental entity of the United States, a State, or political subdivision of a State; or

(2) the reporting of a suspected violation of law to any governmental entity of the United States, a State, or a political subdivision of a State, if such entity has lawful authority with respect to that violation.

§ 1834. Criminal forfeiture and civil ex parte seizure order

(a) Criminal forfeiture - The court, in imposing sentence on a person for a violation of this chapter, shall order, in addition to any other sentence imposed, that he person forfeit to the United States --

(1) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and

(2) any of the person's property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violation, if the court in its discretion so determines, taking into consideration the nature, scope, and proportionality of the use of the property in the offense.

(b) Property subject to forfeiture under this section, any seizure and disposition thereof, and any administrative or judicial proceeding in relation thereto, shall be governed by section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except for subsections (d) and (j) of such section, which shall not apply to forfeitures under this section.

(c) Civil ex parte seizure order – In the case of a civil action arising under 1832(c) of this act, the court may, upon ex parte application, grant an order providing for (i) the seizure of computers or any property used or intended to be used, in any manner or part, to commit or facilitate the commission of such violation, and for (ii) the preservation of evidence in the civil action.

§ 1835. Order to preserve confidentiality

In any such prosecution or 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, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the Unites States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.

§ 1836. Civil proceedings to enjoin violations

(a) The Attorney General may ~~in a civil action,~~ obtain appropriate injunctive relief against any violation of section 1831 of this chapter and the district court of the United States shall have exclusive original jurisdiction of civil actions under section 1831.

~~(b) The district court of the United States shall have exclusive original jurisdiction of civil actions under this subsection~~

(b) Actual or threatened misappropriation may be enjoined.

(c) In appropriate circumstances, affirmative acts to protect a trade secret may be compelled by court order.

(d) If the court determines that it would be unreasonable to prohibit future use, an injunction may condition future use upon payment of a reasonable royalty.

(e) The district courts of the United States shall have original jurisdiction of civil actions under section 1832 of this act.

§ 1837. Applicability to conduct outside the United States

This chapter also applies to conduct outside the Unites States if --

(1) the offender is a natural person who is a citizen or permanent resident alien of the Unites States, or an organization organized under the laws of the Unites States or a State or political subdivision thereof; or

(2) an act in furtherance of the offense was committed in the United States.

§ 1838. Construction with other laws

This chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by the United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret, or to affect the otherwise lawful disclosure of information by any Government employee under section 552 of title 5 (commonly known as the Freedom of Information Act).

§ 1839. Definitions

As used in this chapter --

(1) the term "foreign instrumentality" means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government;

(2) the term "foreign agent" means any officer, employee, proxy, servant, delegate, or representative of a foreign government;

(3) the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if --

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

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

(4) the term "owner", with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed.